

BEST AVAILABLE COPY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-135248

(43)Date of publication of application : 30.04.2004

(51)Int.Cl.

H04L 12/56

H04L 12/46

H04Q 7/38

(21)Application number : 2002-302304

(71)Applicant : FUJITSU LTD

(22)Date of filing : 16.10.2002

(72)Inventor : KAKEMIZU MITSUAKI
YAMAMURA SHINYA
WAKAMEDA HIROSHI
TANIGUCHI HIROYUKI

(30)Priority

Priority number : 2002233622 Priority date : 09.08.2002 Priority country : JP

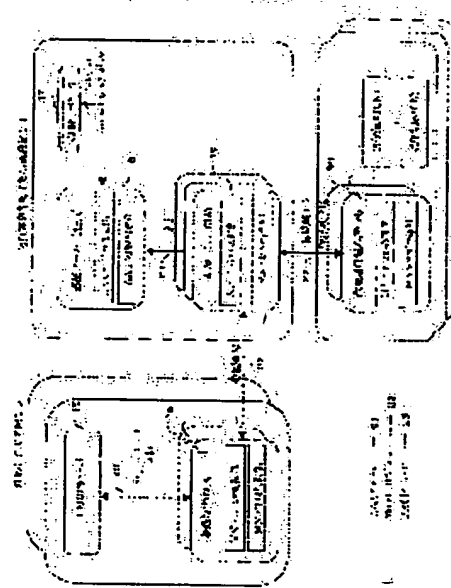
(54) VIRTUAL PRIVATE NETWORK SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a system in which mobile VPN services are safely and seamlessly provided inside and outside an enterprise network without changing a private address assigned on the enterprise network or the like.

SOLUTION: A home agent (HA) is endowed with a gateway function having a security function of the enterprise network. A VPN is established beforehand between the home agent arranged in a communications carrier and a security gateway within the enterprise network, when a service contract is made between the communications carrier and the enterprise. As a result, co-located mode of a mobile node (MN) is used, and VPN information according to a security level of a network that accommodates the mobile node is distributed in a location registration procedure of a mobile IP, so that a VPN that effectively uses a tunnel set-up process of the mobile IP is configured.

本発明の機能ブロック

**LEGAL STATUS**

[Date of request for examination] 17.10.2002

[Date of sending the examiner's decision of rejection] 31.05.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection] 2005-12274

[Date of requesting appeal against examiner's decision of] 30.06.2005

rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-135248

(P2004-135248A)

(43) 公開日 平成16年4月30日(2004.4.30)

(51) Int. Cl.⁷

H04L 12/56

H04L 12/46

H04Q 7/38

F I

H04L 12/56

H04L 12/56

H04L 12/46

H04B 7/26

H04B 7/26

H

100D

V

109M

109A

テーマコード(参考)

5K030

5K033

5K067

審査請求有 請求項の数 10 O L (全 58 頁)

(21) 出願番号 特願2002-302304(P2002-302304)
(22) 出願日 平成14年10月16日(2002.10.16)
(31) 優先権主張番号 特願2002-233622(P2002-233622)
(32) 優先日 平成14年8月9日(2002.8.9)
(33) 優先権主張国 日本国(JP)

(出願人による申告) 国等の委託研究の成果に係る特許出願(平成14年度通信・放送機構「ヒューマンセントリック ユビキタスネットワーク基盤システムに関する研究開発」委託研究、産業活力再生特別措置法第30条の運用を受けるもの)

(71) 出願人 000005223
富士通株式会社
神奈川県川崎市中原区上小田中4丁目1番1号
(74) 代理人 100074099
弁理士 大冢 義之
(74) 代理人 100067987
弁理士 久木元 彰
(72) 発明者 掛水 光明
神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
(72) 発明者 山村 新也
福岡県福岡市早良区百道浜2丁目2番1号
富士通西日本コミュニケーション・システムズ株式会社内

最終頁に続く

(54) 【発明の名称】 仮想閉域網システム

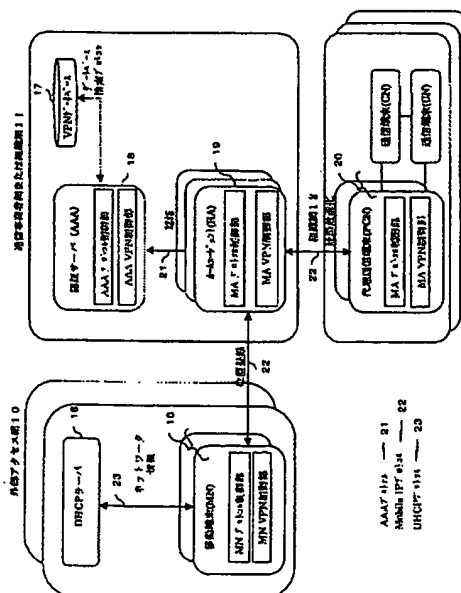
(57) 【要約】

【課題】 企業網などで割り振られたプライベートなアドレスを変更することなく、企業網内外での安全でシームレスなモバイルVPNサービスの提供を可能とするシステムを提供する。

【解決手段】 ホームエージェント(HA)に企業網のセキュリティ機能を持ったゲートウェイ機能を持たせ、通信事業者と企業のサービス契約時に、通信事業者に設置されたホームエージェントと企業網のセキュリティゲートウェイ間に予めVPNを設定することで、移動機(MN)のco-locatedモードを利用し、モバイルIPの位置登録手順の中で移動端末を収容するネットワークのセキュリティレベルに応じたVPN情報を移動端末に配布し、モバイルIPのトンネル設定処理を有効利用したVPNを構成する。

【選択図】 図1

本発明の機能ブロック



【特許請求の範囲】

【請求項 1】

プライベートなネットワークである第1のネットワーク内で使用される第1のアドレスを用いて、第1のネットワークに接続された、第2のアドレスを用いて通信を制御する、第2のネットワークを介した通信を行う仮想閉域網システムであって、
該第1のアドレスを固定的に保持して通信を行う、移動可能な第1の手段と、該第1の手段の第1のアドレスと、第2のネットワークを介した通信を行うための第2のアドレスとの対応関係を取得し、該第1の手段が移動しても通信可能なセッションの確立を行う手順の中で、該第1の手段の認証を行い、該第2のネットワークを介して、第1のネットワークにアクセスする通信装置との間に仮想閉域網を形成する第2の手段と、
を備えることを特徴とする仮想閉域網システム。

【請求項 2】

前記第1の手段が、該第1のネットワークに接続した端末と通信を行う場合に、該第1の手段と該端末との通信経路を最適化する手段を更に備えることを特徴とする請求項1に記載の仮想閉域網システム。

【請求項 3】

前記第2の手段と、前記第1のネットワーク間には、予め仮想閉域網が設定されていることを特徴とする請求項1に記載の仮想閉域網システム。

【請求項 4】

前記移動通信可能なプロトコルは、モバイルIPであることを特徴とする請求項1に記載の仮想閉域網システム。

【請求項 5】

モバイルIPに従って移動端末とプライベートネットワークに接続された端末の通信を可能にするホームエージェントであって、
該移動端末と該ホームエージェントの間に仮想閉域網を設定する手段と、
該移動端末のアクセス認証を行う手段と、
該移動端末に、該認証手段から得られた該仮想閉域網に関する情報を通知する手段と、
を備えることを特徴とするホームエージェント。

【請求項 6】

移動端末とプライベートネットワークに接続された端末の通信を可能にするルータであって、
該移動端末から送られてくる位置登録要求の気付けアドレスまたはドメインを検出する手段と、
検出した該気付けアドレスまたは該ドメインが通信の秘匿性を確保可能な網を示している場合には、該移動端末と該ルータとの間を秘匿性の低い通信プロトコルで、該気付けアドレスが通信の秘匿性を十分保証しきれない網を示している場合には、該移動端末と該ルータとの間を秘匿性の高い通信プロトコルで、該ルータを経由して該移動端末と該端末との通信を行わせる通信制御手段と、
を備えることを特徴とするルータ。

【請求項 7】

移動端末とプライベートネットワークに接続された端末の通信を可能にするルータであって、
該移動端末から送られてくる位置登録要求の気付けアドレスと送信元アドレスを比較する手段と、
該気付けアドレスが所定の通信事業者を示していない場合であって、該気付けアドレスが該送信元アドレスと一致する場合には、該移動端末と該ルータとの間を秘匿性の低い通信プロトコルで、該気付けアドレスが該送信元アドレスと一致しない場合には、該移動端末と該ルータとの間を秘匿性の高い通信プロトコルで、該ルータを経由して該移動端末と該端末との通信を行わせる通信制御手段と、を備えることを特徴とするルータ。

【請求項 8】

プライベートネットワークに接続された端末との通信を可能にする移動端末であって、該移動端末が現在自身の属する網の情報を取得する取得手段と、取得した該網の情報がプライベートネットワークであることを示す場合には、該移動端末の位置を管理するルータのプライベートなアドレスに位置登録要求メッセージを送出し、該網が所定の通信事業者網であることを示す場合には、該ルータのグローバルなアドレスに位置登録要求メッセージを送出し、それ以外の場合には、該ルータのグローバルなアドレスに、秘匿性の高い通信経路の設定要求を含む位置登録要求メッセージを送出するように制御する制御手段と、を備えることを特徴とする移動端末。

【請求項 9】

移動端末とプライベートネットワークに接続された端末の通信を可能にする移動端末であって、該移動端末が現在自身の属する網の気付けアドレスと送信元アドレスを比較する比較手段と、該気付けアドレスが所定の通信事業者のものではない場合であって、該気付けアドレスが該送信元アドレスと一致する場合には、該移動端末とルータとの間を秘匿性の低い通信プロトコルで、該気付けアドレスが該送信元アドレスと一致しない場合には、該移動端末と該ルータとの間を秘匿性の高い通信プロトコルで、該ルータを経由し該移動端末と該端末との通信を行わせる通信制御手段と、を備えることを特徴とする移動端末。

【請求項 10】

移動端末とプライベートネットワークに接続された端末の通信を可能にするシステムにおける移動端末であって、モバイルIPの通信用トンネルを設定する手段と、該モバイルIPの通信用トンネルの設定手順において、該プライベートネットワークの通信用トンネルを形成する手段とを備え、該移動端末は、モバイルIPの通信用トンネルとプライベートネットワークの通信用トンネルを兼用した1つの通信用トンネルを使って通信を行うことを特徴とする移動端末。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、プライベートなネットワークである組織網、と移動端末を収容するネットワーク間の仮想閉域網を実現するためのシステム、移動端末、ホームエージェントおよび通信制御方法に関する。

【0002】

【従来の技術】

近年IMT-2000、ホットスポット、無線LAN等に代表される様々なネットワークによるモバイル環境が整いつつあり、これらのネットワークを通じ企業網に代表されるプライベートなネットワークである組織網へアクセスする機会も増加してきている。

【0003】

外部ネットワークから組織網へアクセスする際、外部ネットワークで割り振られたアドレスを使用し、組織網のセキュリティゲートウェイを経由し通信しているのが一般的である。組織網ではセキュリティを考慮し、アドレスによるフィルタリングを実施している例も少なくない。

【0004】

しかしながら、前述したようなアクセス方法では組織網の内外でアドレスを使い分けている為、必ずしも組織網に直接接続した場合と同様のネットワーク環境が提供されておらず、いい難く、接続状況に関わらずユーザの利便性向上とシームレスで安全な通信が求められている。

【0005】

シームレスな通信を行う手段として、RFC 3220 (IP Mobility Support for IPv4) で規定されたモバイルIPがあるが、同一アドレス体系で運用されるネットワーク内で運用することを前提としており、アドレス体系の異なるネットワーク間での移動は不可能であった。特に、組織網ではプライベートアドレスによる運用が一般的であり、例えばインターネットのような公共ネットワーク内でのルーティングは不可能である。

【0006】

一方、公共ネットワーク内を透過的にプライベートアドレスでルーティングする技術としてRFC 2764 (A Framework for IP Based Virtual Private Networks) で規定された仮想閉域網がある。ここでは、仮想閉域網にホストとホストとの間に設定されるトンネルを含めるものとする。端末の収容先である外部ネットワークで割り振られたアドレスで、組織網に設置したVPNゲートウェイにトンネルを設置し、組織網内の端末と通信を行う方式が一般的である。

【0007】

VPN装置は転送IPパケットにVPNの通信用にRFC 2003 (IP Encapsulation within IP) で規定されるルーティング可能なIPヘッダを付加する機能 (IP in IP) を有し、本来はグローバルアドレスのIPパケットのみしか通らないインターネットに、例えば、プライベートアドレスや、TCP/IPでないプロトコルを利用した通信を可能にすることを、インターネット通信中に別の通信を通すという意味合いから「トンネリング」と呼ばれる。更にトンネリングさせるIPパケットの機密性、安全性を保証するための暗号化と認証を行う技術としてRFC 2401 (Security Architecture for the Internet Protocol) で規定されたIPSecがある。

【0008】

プライベートアドレスによるネットワーク運用が行われている組織網と公共ネットワークを経由したシームレスな通信を行うためには、モバイルIPにおける固定的なアドレスであるホームアドレスに組織網でのプライベートアドレスを適用し、VPNによる公共ネットワーク内をルーティングさせる必要がある。

【0009】

図76、及び図77は、従来の技術における組織網とインターネットのような公共ネットワークを経由したシームレスな通信を行う方法を説明する図である。外部ネットワークとは、インターネットサービスプロバイダ、FOMA、CDMA 2000、ホットスポットに代表される組織網とは異なる組織または事業者によってネットワーク接続サービスが提供されるネットワークである。ここで、ホットスポットとは、無線LANなどで構築された、領域限定の通信ネットワークのことであり、例えば、店舗や企業社屋内などに無線LANなどにより構築されたネットワークである。従って、ホットスポットは、移動通信事業者のサービスの配下にあるが、店舗や企業が移動通信事業者と契約をして、店舗あるいは企業社屋内に限定して構築される。

【0010】

従来においては、図76に示すように、予め組織網のホームエージェント (RFC 3220で規定されるHAであり) と外部ネットワークに設置されたフォーリンエージェント (RFC 3220で規定されるFA) 間でVPNを設定しても移動端末 (RFC 3220で規定されるMN) とフォーリンエージェント (FA) 間をプライベートアドレスによるルーティングが行えない。すなわち、ホームエージェント (HA) とフォーリンエージェント (FA) 間では、プライベートアドレスをルーティングするためのトンネルを張ることができるが、フォーリンエージェント (FA) と移動端末 (MN) の間は、外部ネットワークを介して通信が行われるので、外部ネットワークで移動端末 (MN) に与えられるグローバルなアドレスを使用しなければ、移動端末 (MN) とフォーリンエージェント (FA) が通信できない。

【0011】

そこで、図77に示すようにco-locatedモードサポートによる移動端末(MN)を使用することで、モバイルIPによる位置登録より前にVPNゲートウェイ間にプライベートアドレスによるルーティングを行う為のVPNを設定し、設定したVPNを使用したモバイルIPの位置登録を行う。

【0012】

これにより、ホームエージェント(HA)と移動端末(MN)の間でプライベートアドレスによる通信が可能になる。すなわち、co-locatedモードを利用した場合、最初に移動端末(MN)と、ホームエージェント(HA)を収容するネットワークのゲートウェイ(GW)との間に、トンネリングを利用してVPNが張られ、次に、このVPNを利用してモバイルIPのトンネルをホームエージェント(HA)と移動端末(MN)の間に設定するという2段階のトンネルの設定作業が必要となる。

【0013】

co-locatedモードとは、RFC3220で規定されているモードで、DHCP(Dynamic Host Configuration Protocol)等で移動端末(MN)に割り振られたアドレスを気付アドレス(care of address)とし、移動端末(MN)自身でモバイルIPのトンネル設定を行い、カプセル化及びデカプセル化を行うモードのことである。

【0014】

上記RFC3220では、インターネット上でのモバイルノードへのIPデータグラムをルーティングするプロトコルの改良について記載されている(非特許文献1参照)。

【0015】

また、従来においては、モバイルIPネットワークにおけるVPNシステム及びVPNの設定方法において、モバイルIPにおける位置登録手順と連携してVPN用の特殊な機能を持たせることなく、任意の端末間でのIPSecトンネルによるVPN設定サービスを提供する技術が既にある(特許文献1参照)。

【0016】

【非特許文献1】

Network Working Group, Request for Comments: 3220, Obsoletes: 2002, Category: Standards Track, C. Perkins, Ed, Nokia Research Center, January 2002, "IP Mobility Support for IPv4"

【0017】

【特許文献1】

特開2002-44141号公報

【0018】

【発明が解決しようとする課題】

上述したような方式では、外部ネットワークにフォーリンエージェントを設置した場合、外部ネットワークにおいてプライベートアドレスをルーティングすることができない。一方、co-locatedモードサポートの移動端末を使用した場合、モバイルIPによる通信と、移動端末におけるVPN設定は無関係であり、プライベートアドレスをルーティングさせる為のトンネルとモバイルIPのトンネル設定が必要となる為、モバイルIPによるトンネル設定処理を有効に活かせず、移動端末が移動した際のハンドオーバー処理が効果的でない(ネットワークの切り替えの際、新しいパスの設定に時間がかかるため、スムーズなハンドオーバーが行えない)、またパケット転送においても二重のカプセル化、デカプセル化が必要となる為、スループットが低下する。

【0019】

本発明は、組織網内に設置したホームエージェントに組織網のセキュリティゲートウェイ機能を持たせる、または通信事業者と組織のサービス契約時に、通信事業者網に設置されたホームエージェントと組織網のセキュリティゲートウェイ間に予めVPNを設定するこ

とで、移動端末のco-locatedモードを利用し、モバイルIPの位置登録手順の中で移動端末にVPN情報を配布しモバイルIPのトンネル設定処理を有効利用することで、トンネル設定処理のオーバーヘッドを抑え、公共ネットワークを組織網のプライベートなアドレスでルーティングさせ、プライベートなアドレスのままシームレスで安全な通信を可能にする。

【0020】

本発明の課題は、組織網などで割り振られたプライベートなアドレスを変更することなく、組織網内外でのモバイル環境において安全でシームレスな仮想閉域網サービスの提供を可能とするシステムを提供することである。

【0021】

【課題を解決するための手段】

本発明の仮想閉域網システムは、プライベートなネットワークである第1のネットワーク内で使用される第1のアドレスを用いて、第1のネットワークに接続された、第2のアドレスを用いて通信を制御する、第2のネットワークを介した通信を行う仮想閉域網システムであって、該第1のアドレスを固定的に保持して通信を行う、移動可能な第1の手段と、該第1の手段の第1のアドレスと、第2のネットワークを介した通信を行うための第2のアドレスとの対応関係を取得し、該第1の手段が移動しても通信可能なセッションの確立を行う手順の中で、該第1の手段の認証を行い、該第2のネットワークを介して、第1のネットワークにアクセスする通信装置との間に仮想閉域網を形成する第2の手段とを備えることを特徴とする。

【0022】

本発明のホームエージェントは、モバイルIPに従って移動端末とプライベートなネットワークに接続された端末の通信を可能にするホームエージェントであって、該移動端末と該ホームエージェントの間に仮想閉域網を設定する手段と、該移動端末のアクセス認証を行う手段と、該移動端末に、該仮想閉域網に関する情報を通知する手段とを備えることを特徴とする。

【0023】

本発明の第1のルータは、移動端末とプライベートネットワークに接続された端末の通信を可能にするルータであって、該移動端末から送られてくる位置登録要求の気付けアドレスまたはドメインを検出する手段と、検出した該気付けアドレスまたは該ドメインが通信の秘匿性を確保可能な網を示している場合には、該移動端末と該ルータとの間を秘匿性の低い通信プロトコルで、該気付けアドレスが通信の秘匿性を十分保証しきれない網を示している場合には、該移動端末と該ルータとの間を秘匿性の高い通信プロトコルで、該ルータを経由して該移動端末と該端末との通信を行わせる通信制御手段とを備えることを特徴とする。

【0024】

本発明の第2のルータは、移動端末とプライベートネットワークに接続された端末の通信を可能にするルータであって、該移動端末から送られてくる位置登録要求の気付けアドレスと送信元アドレスを比較する手段と、該気付けアドレスが所定の通信事業者を示していない場合であって、該気付けアドレスが該送信元アドレスと一致する場合には、該移動端末と該ルータとの間を秘匿性の低い通信プロトコルで、該気付けアドレスが該送信元アドレスと一致しない場合には、該移動端末と該ルータとの間を秘匿性の高い通信プロトコルで、該ルータを経由して該移動端末と該端末との通信を行わせる通信制御手段とを備えることを特徴とする。

【0025】

本発明の第1の移動端末は、プライベートネットワークに接続された端末との通信を可能にする移動端末であって、該移動端末が現在自身の属する網の情報を取得する取得手段と、取得した該網の情報がプライベートネットワークであることを示す場合には、該移動端末の位置を管理するルータのプライベートなアドレスに位置登録要求メッセージを送出し、該網が所定の通信事業者網であることを示す場合には、該ルータのグローバルなアドレ

スに位置登録要求メッセージを送出し、それ以外の場合には、該ルータのグローバルなアドレスに、秘匿性の高い通信経路の設定要求を含む位置登録要求メッセージを送出するように制御する制御手段とを備えることを特徴とする。

【0026】

本発明の第2の移動端末は、移動端末とプライベートネットワークに接続された端末の通信を可能にする移動端末であって、該移動端末が現在自身の属する網の気付けアドレスと送信元アドレスを比較する比較手段と、該気付けアドレスが所定の通信事業者のものではない場合であって、該気付けアドレスが該送信元アドレスと一致する場合には、該移動端末とルータとの間を秘匿性の低い通信プロトコルで、該気付けアドレスが該送信元アドレスと一致しない場合には、該移動端末と該ルータとの間を秘匿性の高い通信プロトコルで、該ルータを経由し該移動端末と該端末との通信を行わせる通信制御手段とを備えることを特徴とする。

【0027】

本発明の第3の移動端末は、移動端末とプライベートネットワークに接続された端末の通信を可能にするシステムにおける移動端末であって、モバイルIPの通信用トンネルを設定する手段と、該モバイルIPの通信用トンネルの設定手順において、該プライベートネットワークの通信用トンネルを形成する手段とを備え、該移動端末は、モバイルIPの通信用トンネルとプライベートネットワークの通信用トンネルを兼用した1つの通信用トンネルを使って通信を行うことを特徴とする。

【0028】

本発明によれば、ホームアドレスとしての不変的でプライベートなアドレスである第1のアドレスと気付けアドレスである通信可能な第2のアドレスの対応をとり、移動端末のローミングを可能にする過程で、移動端末とホームエージェントの間で仮想閉域網の情報を交換し、仮想閉域網を設定することにより、モバイルIPの確立と仮想閉域網の確立の手順を簡素化し、従来2重のカプセル化が必要であるために、不具合を生じていたハンドオーバーなどの時においても、迅速に移動端末への仮想閉域網の設定を行うことができる。

【0029】

【発明の実施の形態】

システム機能概要

図1は、本発明の機能ブロックである。

【0030】

以下に機能概要を述べる。

組織網11、12

組織網11、12は、企業、大学、官庁のような組織内に閉じたプライベートなネットワークであり、例えばインターネットのような公共ネットワークとはファイアーウォール(firewall)を介して接続される。組織網内で使用されるアドレス形態はプライベートアドレス(private address)でもグローバルアドレス(global address)どちらもよいが、組織網内のみで通信可能と言う意味で本発明では「プライベートなアドレス」と呼ぶことにする。一方、公共ネットワークで通信可能なアドレスを「グローバルなアドレス」と呼ぶこととする。従って、モバイルIPプロトコルにおいては「プライベートなアドレス」は固定的な第1のアドレスにあたるホームアドレス(home address)となり、「グローバルなアドレス」は通信可能な第2のアドレスである気付アドレス(care of address)となる。

【0031】

以降、本発明の実施形態を説明する上で、組織網の代表例として企業網を取り上げて説明する。

なお、図1において、ホームエージェント19は、通常複数個設けられ、一つの組織網12を複数のホームエージェント19で分散処理すると共に、このような複数のホームエージェント19の集合が、異なる組織網12毎にそれぞれ設けられる構成が採られる。

認証サーバ18

認証サーバ18は、認証 (Authentication)、認可 (Authorization)、課金 (Accounting) を行うサーバ群の IETF で用いられる名称 (以降、AAA) である。上記機能に加え、VPN データベース17から認証要求をしてきたユーザのVPN情報を抽出し、HA19へAAAプロトコル21を用いてVPN情報を通知するAAAプロトコル制御部とユーザ単位のVPN情報の抽出とVPN経路の決定を行うAAAVPN制御部から構成される。図1においては、通信事業者網または企業網11に設けられている。

AAAプロトコル21

AAAシステムが使用するプロトコルを示す。AAAプロトコルは認証、認可、課金、ポリシーに関する情報を伝達可能なあらゆるプロトコルで実装可能である。本発明の実施形態では、使用するプロトコルを特定しないが、仮に現在 IETF で検討中の DIAMETER プロトコルの使用を想定する。本発明の実施形態で必要となる新たな情報の伝達には、DIAMETER プロトコルで定義される AVP (Attribute Value Pair) と呼ばれる拡張可能な属性パラメータを用いる。拡張される属性は、VPN 設定に関する情報である。

データベース検索プロトコル

VPN データベース17を検索するためのプロトコルである。使用するプロトコルはVPN データベース17を実装するデータベースの製品に依存する。LDAP (Light Directory Access Protocol) やSQLが通常用いられる。本発明の実施形態では、検索プロトコルとデータベースの動作については限定しない。VPN データベース17

図13は、本発明の実施形態で使用するVPNデータベース17の構成の例を示す図である。

【0032】

VPN データベース17は、各ユーザの設定したVPNデータインスタンスの集合であり、各インスタンスが一つのVPNに対応する。各VPNデータインスタンスは、このVPN情報を一意に表す識別子であるプロファイル番号 (Profile Number)、ユーザのネットワーク識別子 (Nai)、セキュリティゲートウェイ間の共有のセキュリティ関係を使用するか、ユーザ固有のセキュリティ関係を使用するかを示すVPN共有指標 (vpns share)、VPN種別 (vpn kind)、通信先端末のIPアドレス (dest addr)、上り方向のQoSクラス (up class)、下り方向のQoSクラス (down class)、IPSecで使用する上り方向SPI (up SPI)、IPSecで使用する下り方向SPI (down SPI)、UDPカプセル化で使用するIPのポート番号 (port Number) で構成される。

【0033】

共有指標に0が設定された場合、up class、down class、up SPI、Down SPIは省略可能である。このデータベースはユーザのNAIで検索され、検索された全てのインスタンスは、後述するVPN情報キャッシュにアドレス情報を付加して記録される。

DHCPプロトコル23

RFC2131と将来の変更で規定される全ての端末のネットワーク設定プロトコルを示す。移動端末 (MN16) はDHCPREQUESTメッセージを使用し、外部アクセス網10であるネットワークに設けられるDHCPサーバ15に対しネットワーク情報を要求し、DHCPサーバ15は、DHCPACKメッセージを使用し、移動端末 (MN16) にネットワーク情報を指示する。DHCPACKメッセージで通知されるネットワーク情報には、移動端末 (MN16) のIPアドレス、ネットマスク、ゲートウェイアドレス、ドメイン名、DNSアドレス等がある。本発明の実施形態では、移動端末 (MN16) のアドレス取得手段としてDHCPプロトコルを想定しているが、ネットワークからIPアドレスを取得することができるプロトコルならば特に限定はしない。

モバイルIPプロトコル22

RFC 3220と将来の変更で規定される全てのモバイルIPプロトコルを示す。

【0034】

図2～図12は、DIAMETERプロトコルの詳細を示す図である。

図2及び図3は、モバイルIPメッセージとDIAMETERメッセージの構成を示す図である。両メッセージにおいて、IPヘッダとUDPヘッダは共通である。図2(a)のモバイルIPメッセージとDIAMETERメッセージのそれぞれのヘッダやAVPのフォーマットは、図2(b)～図3(c)に記載した構成となっている。

【0035】

また、図4は、モバイルIPの位置登録要求(Reg. Request)メッセージ構成であり、図5は、DIAMETERの認証要求(AMR: AA Mobile Node Request)メッセージの構成であり、図6は、DIAMETERのホームエージェント登録要求(HAR: Home Agent MIP Request)メッセージの構成である。

【0036】

図7及び図8は、モバイルIPの位置登録応答(Reg. Reply)メッセージの構成を示し、図9(a)は、DIAMETERの認証応答(AMA: AA Mobile Node Answer)メッセージの構成、図9(b)は、DIAMETERのホームエージェント登録応答(HAA: Home Agent MIP Answer)メッセージの構成を示す。

【0037】

図10及び図11は、CN方向からMN方向へのパケットを、HAを介さず直接MNへ送信する為の経路最適化を目的としたモバイルIPの結合更新(BU: Binding Update)メッセージの構成を示し、図12は、モバイルIPの結合応答(BA: Binding Acknowledge)メッセージの構成を示している。

ホームエージェント(HA) 19

RFC 3220で定義されるモバイルIPプロトコル22手順を用いて移動端末(MN 16)の位置を管理する機能(以降HA)である。また、ホームエージェントを移動通信制御装置あるいはルータと呼ぶことがある。

本発明の実施形態のネットワーク装置は通信事業者網内または企業網内11のセキュリティゲートウェイとして設置される。ホームエージェント(HA 19)は企業網12で割り付けられたプライベートなアドレスをホームアドレスとして所有するエージェントであり、ホームエージェント(HA 19)に送信されてきた移動端末(MN 16)のホームアドレスを送信先とするパケットはホームアドレスに対応した移動端末(MN 16)の気付アドレス(care of address)へカプセル化されて送出される。このアドレスの対応は、移動結合と呼ばれるテーブルで管理される。また、HA 19は、位置登録応答(Reg. Reply)メッセージにサービスプロファイルを設定することによりVPN情報を移動端末(MN 16)に通知する。本発明の実施形態のHA 19はIP in IP、IPSec、IPSec+UDP(NAT(Network Address Translation)/NAPT(Network Address Port Translation)のアドレス変換及びポート番号変換されたパケットに対応する為、UDP in IPカプセル化実施後IPSecカプセル化を行う)のVPNゲートウェイ機能、及びAAAプロトコルとモバイルIPプロトコルで通知されるVPN情報を解析するMAプロトコル制御部(モバイルエージェントプロトコル制御部)と、解析したVPN情報に基づきネットワークカーネルに指定されたセキュリティレベルでのトンネル設定を行うMAVPN制御部(モバイルエージェントVPN制御部)を有する。

代理通信装置(PCN) 20

モバイルIPプロトコル22の移動結合の更新処理でホームエージェント(HA 19)から通知された送信先へ、VPNを設定するネットワーク機能(以降PCN: Proxy Correspondent Node)である。ホームエージェント(HA 19)からの結合更新(BU)メッセージを利用し、企業網内折り返し、及び、PCN-PCN間

のトンネル設定を行うことで、移動端末(MN16)への経路最適化を行う。本発明の実施形態のPCNはIPinIP、IPSec、IPSec+UDPのセキュリティゲートウェイ機能を兼ね、モバイルIPプロトコルで通知されるVPN情報を解析するMAプロトコル制御部と、解析したVPN情報に基づきネットワークカーネルに指定されたセキュリティレベルでのトンネル設定を行うMAVPN制御部を有する。図1では、PCN20は、企業網12に設けられている。

移動端末(MN)16

本発明の実施形態のネットワーク装置である移動端末(MN16)は、モバイルIPプロトコル22手順を用いてセッションを維持したままネットワーク内を移動できるRFC3220で定義される機能(以降MN)である。本発明の実施形態の移動端末(MN16)は、IPinIP、IPSec、IPSec+UDPのトンネリング機能を有し、暗号化/復号化及びカプセル化/デカプセル化を行う。移動端末(MN16)は気付アドレス(care of address)へカプセル化されて送出されてきたパケットをデカプセル化し、ホームアドレスに対応したアプリケーションへパケットを通知する。また、アプリケーションからホームアドレスで通知されたユーザパケットを気付けアドレスでカプセル化し、通信端末(CN)へパケットを送出する。ホームエージェント(HA19)からの位置登録応答(Reg. Reply)メッセージで通知されたサービスプロファイルのセキュリティレベルに応じて、通常のIPinIPトンネルの他にIPSec、IPSec+UDPトンネルを設定し、移動端末(MN16)からホームエージェント(HA19)へのトンネル(通常リバーストンネルと呼ばれる)にも同様のトンネルを設定する。モバイルIPプロトコルで通知されるVPN情報を解析するMNプロトコル制御部と、解析したVPN情報に基づきネットワークカーネルに指定されたセキュリティレベルでのトンネル設定を行うMNVN制御部を有する。本発明ではモバイルIPプロトコルによる通信可能なノートパソコンを例に説明を行う。

【0038】

図14～図20は、図1～図13で説明した機能を持つ認証サーバ及びネットワーク装置で構成されるIPネットワーク構成を示す図である。

図14は、プライベートなアドレスで運用される企業網と、グローバルなアドレスで運用される公共ネットワーク(例えば、インターネット)と、企業網との相互接続契約に基づき網接続端末へグローバルなアドレスを付与し、企業網へのアクセス手段を提供するアクセス網とで構成されるネットワークを基本にしている。

【0039】

そして、図14のシステムは、企業網内のプライベートなアドレスをモバイルIPプロトコルにおける不変的なアドレスであるホームアドレス(home address)として持ち、企業内及び外部ネットワークのアクセス網間においてプライベートなアドレス(home address)を保持したまま移動し、企業網と通信を継続する移動端末(MN)と、企業内にあって移動端末(MN)を認証する認証サーバ(AAA)、企業内にあって移動端末(MN)の位置管理を行うホームエージェント(HA)で構成されたシステムである。

【0040】

図15は、プライベートなアドレスで運用される企業網と、グローバルなアドレスで運用される公共ネットワーク(例えば、インターネット)と、企業網との相互接続契約に基づき網接続端末へグローバルなアドレスを付与し企業網へのアクセス手段を提供するアクセス網とで構成されるネットワークを基本にしている。

【0041】

そして、図15のシステムは、企業網内のプライベートなアドレスをモバイルIPプロトコルにおける不変的なアドレスであるホームアドレス(home address)として持ち、企業内及び外部ネットワークのアクセス網間をプライベートなアドレス(home address)を保持したまま移動し、企業網と通信を継続する移動端末(MN)と、企業内にあって移動端末(MN)を認証する認証サーバ(AAA)、企業網のセキュリ

ティゲートウェイにあって移動端末(MN)の位置管理を行うホームエージェント(HA)、企業網内についてホームエージェント(HA)からの結合更新メッセージを利用し、企業網内にあって経路最適化を行う代理通信装置(PCN)で構成されたシステムである。

【0042】

図16は、プライベートなアドレスで運用される企業網と、グローバルなアドレスで運用される公共ネットワーク(例えば、インターネット)と、企業網との相互接続契約に基づき網接続端末へグローバルなアドレスを付与し企業網へのアクセス手段を提供するアクセス網とで構成されるネットワークを基本としている。

【0043】

そして、図16のシステムは、企業網内のプライベートなアドレスをモバイルIPプロトコルにおける不変的なアドレスであるホームアドレス(home address)として持ち、企業内及び外部ネットワークのアクセス網間においてプライベートなアドレス(home address)を保持したまま移動し、企業網と通信を継続する移動端末(MN)と、企業内にあって移動端末(MN)を認証する認証サーバ(AAA)、企業網のセキュリティゲートウェイにあって移動端末(MN)の位置管理を行うホームエージェント(HA)、企業網内にあってホームエージェント(HA)からの結合更新メッセージを利用し、企業網内にあって経路最適化を行う代理通信装置(PCN)で構成されるシステムである。HA-PCN間は、サービス開始時、セキュリティを考慮し、IPSec(IE TFによって標準化されているパケットの暗号化と認証技術)によるトンネルを設定しておく。

【0044】

図17は、プライベートなアドレスで運用される企業網と、グローバルなアドレスで運用される公共ネットワーク(例えば、インターネット)と、企業網との相互接続契約に基づき網接続端末へグローバルなアドレスを付与し企業網へのアクセス手段を提供する通信事業者網とで構成されるネットワークを基本としている。

【0045】

そして、図17のシステムは、企業網内のプライベートなアドレスをモバイルIPプロトコルにおける不変的なアドレスであるホームアドレス(home address)として持ち、企業内及び外部ネットワークのアクセス網をプライベートなアドレスを保持したまま移動し、企業網と通信を継続する移動端末(MN)と、通信事業者網にあって移動端末(MN)を認証する認証サーバ(AAA)、通信事業者網にあって移動端末(MN)の位置管理を企業網内のプライベートなアドレスで行うホームエージェント(HA)と、企業網にあって企業網とホームエージェント(HA)間において公共ネットワークを介してVPNで結ぶためのゲートウェイ装置と、企業網のセキュリティゲートウェイにあって、ホームエージェント(HA)の指示により企業網に在圏する移動端末(MN)への通信を企業網内で折り返す代理通信装置(PCN)とで構成されるシステムである。HA-PCN間はサービス開始時、セキュリティを考慮し、IPSecによるトンネルを設定しておく。

【0046】

図18は、プライベートなアドレスで運用される企業網と、グローバルなアドレスで運用される公共ネットワーク(例えば、インターネット)と、企業網との相互接続契約に基づき網接続端末へグローバルなアドレスを付与し企業網へのアクセス手段を提供する通信事業者網とで構成されるネットワークを基本としている。

【0047】

そして、図18のシステムは、企業網内のプライベートなアドレスをモバイルIPプロトコルにおける不変的なアドレスであるホームアドレス(home address)として持ち、企業内及び外部ネットワークのアクセス網間をプライベートなアドレスを保持したまま移動し、企業網と通信を継続する移動端末(MN)と、通信事業者網にあって移動端末(MN)を認証する認証サーバ(AAA)、通信事業者網にあって移動端末(MN)の位置管理を企業網内のプライベートなアドレスで行うホームエージェント(HA)と、企

業網にあって企業網とホームエージェント（HA）間において公共ネットワークを介してVPNで結ぶためのゲートウェイ装置と、通信事業者網とのゲートウェイにあって、ホームエージェント（HA）の指示により企業網に在圏する移動端末（MN）への通信を企業網内で折り返す代理通信装置（PCN）とで構成されるシステムである。HA-PCN間はサービス開始時、セキュリティを考慮し、IPSecによるトンネルを設定しておく。

【0048】

図19は、プライベートなアドレスで運用される企業網と、グローバルなアドレスで運用される公共ネットワーク（例えば、インターネット）と、企業網との相互接続契約に基づき網接続端末へグローバルなアドレスを付与し企業網へのアクセス手段を提供する通信事業者網とで構成されるネットワークを基本としている。

【0049】

そして、図19のシステムは、企業網内のプライベートなアドレスをモバイルIPプロトコルにおける不変的なアドレスであるホームアドレス（home address）として持ち、企業内及び外部ネットワークのアクセス網間をプライベートなアドレスを保持したまま移動し、企業網と通信を継続する移動端末（MN）と、通信事業者網にあって移動端末（MN）を認証する認証サーバ（AAA）、通信事業者網にあって移動端末（MN）の位置管理を企業網内のプライベートなアドレスで行うホームエージェント（HA）と、企業網にあって企業網とホームエージェント（HA）間において公共ネットワークを介してVPNで結ぶためのゲートウェイ装置と、企業網内にあって、ホームエージェント（HA）の指示により企業網に在圏する移動端末（MN）への通信を企業網内で折り返す代理通信装置（PCN）とで構成されるシステムである。HA-PCN間はサービス開始時、セキュリティを考慮し、IPSecによるトンネルを設定しておく。

【0050】

図20は、プライベートなアドレスで運用される企業網と、グローバルなアドレスで運用される公共ネットワーク（例えば、インターネット）と、企業網との相互接続契約に基づき網接続端末へグローバルなアドレスを付与し企業網へのアクセス手段を提供する通信事業者網とで構成されるネットワークを基本としている。

【0051】

そして、図20のシステムは、企業網内のプライベートなアドレスをモバイルIPプロトコルにおける不変的なアドレスであるホームアドレス（home address）として持ち、企業内及び外部ネットワークのアクセス網間をプライベートなアドレスを保持したまま移動し、企業網と通信を継続する移動端末（MN）と、通信事業者網にあって移動端末（MN）を認証する認証サーバ（AAA）、通信事業者網にあって移動端末（MN）の位置管理を企業網内のプライベートなアドレスで行うホームエージェント（HA）と、企業網にあって企業網とホームエージェント（HA）間において公共ネットワークを介してVPNで結ぶためのゲートウェイ装置と、企業網外にあって、ホームエージェント（HA）の指示により企業網に在圏する移動端末（MN）への通信を企業網内で折り返す代理通信装置（PCN）とでシステムを構成する。HA-PCN間はサービス開始時、セキュリティを考慮し、IPSecによるトンネルを設定しておく。

機能エンティティ詳細説明

AAA

図21は、図1のAAA18の機能ブロックを示す図の例である。

【0052】

AAAは、AAAプロトコル制御部30、AAAVPN制御部31、データベースサーバ32、ネットワークカーネル33、ネットワークデバイスインタフェース34から構成される。

【0053】

AAAプロトコル制御部30は、AAAプロトコルを制御するAAAプロトコル処理部35から構成される。

AAAVPN制御部31は、VPNデータベースより抽出したVPN情報をキャッシュす

るVPN情報キャッシュ36（図22）、鍵生成器37から構成される。この鍵生成器37によって生成された鍵は、形成されたVPNを通るデータを暗号化するなどのために使用される。

【0054】

図22は、VPN情報キャッシュの構成を示す図の例である。

例えば、VPN情報キャッシュは、VPN情報キャッシュインスタンスの集まりであり、ユーザがネットワークにアクセスしている間有効なネットワークで一意なユーザに固有な情報を含むセッションIDで検索される。VPN情報キャッシュインスタンスは一意な識別子であるセッションID、このユーザが設定しているVPNの数を示すプロファイル数、各VPNの設定情報を含むVPN情報プロファイルから構成される。VPN情報プロファイルは、VPNを一意に識別する識別子であるプロファイル番号、VPN適用のパケットを特定するための送信元と宛先のIPアドレスとそのネットマスク、パケットに設定するTOS値、IPSecをAH（Authentication Header Protocol）、ESP（Encapsulating Security Payload）、カプセル化のみのいずれかで設定するかを示すセキュリティタイプ、IPSecトンネルモードで参照されるIPSecトンネルの入口と出口である送信元と宛先のゲートウェイアドレス、宛先ゲートウェイが動的なVPN設定が可能かどうかを示す宛先GW種別、上りと下り方向のセキュリティ関係の識別子であるSPI（Security Parameter Index）、ESP暗号鍵、ESP認証鍵で構成される。

【0055】

データベースサーバ32は、VPNデータベース（図13）とWEBアプリケーションから構成される。

ネットワークカーネル33はIPパケットの転送とネットワークへの接続点である物理インタフェースを制御するオペレーティングシステムであり、IPパケット転送のルートを決めるルーティングテーブル（図23）を持つ。ネットワークカーネルはIPパケットのカプセル化、パケット編集、パケット送出のキュー制御等を行うが、これらの機能はオペレーティングシステム依存であり、本発明の実施形態では限定しない。

【0056】

図23は、ルートテーブルの構成を示す図の例である。一般的なルーティングテーブルは、送信先アドレス、ゲートウェイアドレス、ネットマスク、メトリック、出カインタフェースから構成されており、送信先アドレスとメトリックで転送先ネットワークノードが決定される。本発明の実施形態はルートテーブルの構成には依存しないが、出力先に仮想ネットワークデバイスインタフェースを設定できるようなネットワークカーネルを例に以降の具体的な説明を行う。

【0057】

又、ネットワークカーネル33はカプセル化されたパケットを受信すると、パケットをデカプセル化する機能を持っており、デカプセル後のパケットがESPヘッダを含んでいれば、トンネル制御部で保持しているESP情報を参照して暗号化されたパケットをデコードする機能を持つ。更にIPSecデカプセル化したデータがUDP（User Datagram Protocol）フォーマットの場合、UDPデカプセル化を行う。これらの機能はカプセル化、IPSecそのものの実装に依存する部分であり、本質ではないため、概略のみを説明するに留める。

【0058】

ネットワークデバイスインタフェース34はネットワークデバイスへのインタフェースである。ネットワークデバイスインタフェース34には、実装方法により、物理ネットワークデバイスインタフェースと仮想ネットワークデバイスインタフェースがある。

【0059】

物理ネットワークデバイスインタフェースは、例えばLAN、ISDN、ATM等のインタフェースカードである。物理ネットワークデバイスインタフェースの制御ドライバを「実デバイス」と呼ぶ。

【0060】

仮想ネットワークデバイスインタフェースは仮想のネットワークデバイスへのインタフェースであり、物理ネットワークデバイスインタフェースと同様の制御により、ソフトウェア実装によるトンネリングやIPSecなどの機能を実現する、仮想のインターフェースカードである。トンネリングなどのある機能を持った仮想ネットワークインタフェースのドライバを「仮想デバイス」と呼ぶ。ネットワークカーネル33がルーティングテーブルを参照し、仮想デバイスとパケットの送受信を行うことでカプセル化／デカプセル化などが行われる。本発明の説明ではIPinIPは仮想デバイスtunnel、IPSec、IPSec+UDPは仮想デバイスipseccで実装されている。もちろん、このような機能はハードウェア（物理ネットワークデバイスインタフェース）で実装しても構わない。

【0061】

図24から図26はAAAの処理フローである。以下、これらのフローを用いてAAAの処理を説明する。

図24は、AAAの全体処理フローの例である。

【0062】

S100：ネットワークカーネル33は物理ネットワークインタフェース34よりパケットを受信すると、IPのポート番号を検索することによりAAAプロトコルシグナリングパケット（DIAMETER）を選択し、AAAプロトコル制御部30に受信パケットの情報を渡す。

【0063】

図25は、図21内に示されるAAAプロトコル制御部30の処理フローの例である。

S110：AAAプロトコル制御部30内のAAAプロトコル処理部35はネットワークカーネル33から受信したAAAプロトコル（DIAMETER）のコマンドコードAVPより受信メッセージを判定する。AMR（AAMobile Node Request）であればS111へ、HAA（Home Agent MIP Answer）であればS114へ処理を分岐する。

S111：AMRを受信したAAAプロトコル処理部35はAAAVPN制御部31を起動する。

S112：AAAVPN制御部31はデータベースサーバ32内にあるVPNデータベースからVPN情報を読み出し、VPN情報キャッシュ36に設定する。

S113：AAAプロトコル処理部35はVPN情報としてSPC固定部（図7）にサービスプロファイルを設定したモバイルIPプロトコルの位置登録要求メッセージ（Reg. Request）をAAAプロトコルのホームエージェント登録要求メッセージ（HAR：Home Agent MIP Request）に設定する。

S114：HAAを受信したAAAプロトコル処理部35はAAAVPN制御部31を起動し、AAAVPN制御部31はモバイルIPプロトコルの位置登録要求メッセージ（Reg. Request）を使って位置登録を要求してきたMNの正当性を保証する為の認証子を生成する。

S115：AAAプロトコル処理部35はSPC固定部（図7）にVPN情報を設定したモバイルIPプロトコルの位置登録応答メッセージ（Reg. Reply）に認証子を付加し、認証応答メッセージ（AMA）に設定する。

S116：AAAプロトコル制御部30はHAA宛に認証応答メッセージ（AMA）メッセージ、またはホームエージェント登録要求メッセージ（HAR）を送出する。

【0064】

図26は、図21内に示されるAAAVPN制御部31の処理フローの例である。図25のS112の処理時に起動される。

S120：AAAVPN制御部31はSQL等のデータベースアクセス言語を用いて、MNのNetwork Access Identifier（NAI）でデータベースサーバ32に問い合わせ、データベースサーバ32はVPNデータベースから対応するVPN

情報を読み出す。

S121: AAAVPN制御部31はデータベースサーバ32内にあるVPNデータベースより読み出したSPI (Security Parameter Index) が、デフォルトSPIであれば無処理のままS112へ処理を分岐する。そうでなければS122へ処理を分岐する。デフォルトSPIは予めAAA内に初期構成時に設定されている、又はAAAのローカルな保守コンソールから設定されているものとする。

S122: AAAVPN制御部31は鍵生成器37を起動する。鍵生成器37はVPNデータベースから読み出したVPN情報の設定鍵長に従い、乱数を生成する。

【0065】

図27は、図1のHA19、PCN20であるモバイルエージェント(MA)の機能ブロックを示す図の例である。モバイルIPのプロトコルを処理するプロセスあるいはエージェントを総称してモバイルエージェント(MA)と呼ぶ。

【0066】

これらのネットワーク装置は、MAプロトコル制御部40、MAVPN制御部41、ネットワークカーネル42、ネットワークデバイスインタフェース43から構成される。

【0067】

MAプロトコル制御部40は、AAAプロトコルを制御するAAAプロトコル処理部44とモバイルIPを制御するモバイルIPプロトコル処理部45から構成される。

【0068】

MAVPN制御部41は、AAAプロトコル、モバイルIPプロトコルにより通知されたVPN情報をキャッシュするVPN情報キャッシュ46(図22)、トンネル制御部47から構成される。

【0069】

トンネル制御部47は、VPN情報キャッシュ46に設定されたVPN種別に応じて送信先のIPアドレスに対してルートテーブルの出力デバイスを書き換える。IP in IPの場合トンネル仮想デバイスに、IPSec または IPSec + UDP の場合 ipsec 仮想デバイスに書き換える。またVPN情報テーブル48(図28)にVPN種別、送信元と送信先のIPアドレスとそのネットマスク、セキュリティタイプ、送信元と送信先のゲートウェイアドレス、上りと下り方向のセキュリティ関係の識別子であるSPI (Security Parameter Index)、ESP暗号鍵、ESP認証鍵、UDPカプセルを行う際のIPのポート番号(port Number)を設定する。ネットワークカーネル42により仮想デバイスに出力されたパケットはVPN情報テーブル48を参照して、暗号化/復号化とカプセル化/デカプセル化が実行される。

【0070】

図28は、VPN情報テーブルを示す図の例である。

例えば図28に示すVPN情報テーブルは、IPSec情報、ESP情報、トンネル情報で構成される。IPSec情報はIPSec情報インスタンスの集まりであり、送信元アドレスと宛先アドレスの組で特定される。IPSec情報インスタンスは送信元アドレス/ネットマスク、宛先アドレス/ネットマスク、パケットの実際の転送先である実宛先アドレス、このパケットに適用するトンネル情報の識別子、このパケットに適用するESP情報の識別子から構成される。ESP情報はESP情報インスタンスの集まりであり、ESP情報を一意に識別するESP識別子、暗号化手法、方向、AH認証鍵長、ESP認証鍵長、ESP暗号鍵長、AH認証鍵、ESP認証鍵、ESP暗号鍵で構成される。トンネル情報はトンネル情報インスタンスの集まりであり、トンネル情報を一意に識別するトンネル識別子、カプセル化手法、方向、トンネルの入口と出口になる送信元アドレスと宛先アドレスから構成される。

【0071】

VPN情報キャッシュ46、ネットワークカーネル42、ネットワークデバイスインタフェース43はAAAの詳細説明の中で既に述べた。

図29から図35は、MA(Mobile Agent)の処理フローである。以下、こ

これらのフローを用いてMAの処理を説明する。なお、ここでは、モバイルIPのプロトコルを処理するプロセスあるいはエージェントを総称してモバイルエージェントと呼んでいる。

【0072】

図29は、MAの全体処理フローの例である。

S200：ネットワークカーネル42はネットワークデバイスインタフェース43よりパケットを受信すると、既に概略を説明したようにデカプセル化、暗号復号化を行った後、パケットがシグナリングパケットかデータパケットかで切り分ける。

シグナリングパケットであるかどうかはMAプロトコル制御部40が指定したポート番号でパケットを受信したかどうかで決定される。シグナリングパケットであればS201、それ以外であればS203へ処理を分岐する。

S201：MAプロトコル制御部40へ受信パケットの情報を渡し、ポート番号によりAAAとのAAAプロトコル及びMNとのモバイルIPプロトコルの処理を行う。

S202：MAプロトコル制御部40はMAVPN制御部41を起動し、VPN情報の設定を行う。

S203：ネットワークカーネル42は受信パケットの出力先のインタフェースを、ルーティングテーブルを参照して決定する。出力先が仮想デバイスであればカプセル化や暗号化が行われ、再度ネットワークカーネル42はカプセル化した宛先でルーティングテーブルを参照し、出力デバイスを決定する。出力先が物理デバイスであれば、そのデバイスへパケットを送信する。

図30は、図27内に示されるMAプロトコル制御部40の処理フローの例である。

S210：図27内に示されるMAプロトコル制御部40はネットワークカーネル2から受信したパケットのIPのポート番号を調べ、AAAプロトコルのポート番号であればS211へ、モバイルIPプロトコルであればS212へ処理を分岐する。

S211：AAAプロトコル処理部44を起動し、AAAプロトコルの処理後、AAAプロトコルに情報の一部として付加されているモバイルIPプロトコルを取り出しS212へ処理を渡す。

S212：モバイルIPプロトコル処理部45を起動し処理を終了する。

図31は、図27内に示されるAAAプロトコル処理部44の処理フローの例である。

S220：AAAプロトコル処理部44はネットワークカーネル42から受信したAAAプロトコルよりVPN情報を抽出し、MAVPN制御部41を起動する。MAVPN制御部41は、AAAプロトコル処理部44にて抽出されたVPN情報をVPN情報キャッシュ46へ設定する。後述のモバイルIPプロトコル処理部が参照するために、キャッシュの設定、更新を行った場合、共有メモリ上に更新したことを示すフラグを立てる。

S221：AAAプロトコルの処理後、AAAプロトコルに情報の一部として付加されているモバイルIPプロトコルを取り出す。

【0073】

図32は、図27内で示されるモバイルIPプロトコル処理部45の処理フローの例である。

S230：受信したモバイルIPプロトコルメッセージのタイプを判定する。タイプが位置登録要求(Reg. Request)であればS231へ、登録要求(BU: Binding Update)、登録応答(BA: Binding Ack)であればS235へ処理を分岐する。

位置登録要求(Reg. Request)の場合：

S231：登録要求を受信したモバイルエージェント(MA)がホームエージェント(HA)の場合、モバイルIPプロトコル処理部45は登録要求メッセージの気付アドレス(care of address)と移動性結合内の旧気付アドレスを比較し、比較結果が異なればS232へ処理を分岐する。

S232：モバイルIPプロトコル処理部45はAAAプロトコル処理部44で認証応答メッセージ(AMA)で通知されたVPN情報をMAVPN制御部41に通知すると、M

AVPN制御部41はVPN情報キャッシュを通知されたVPN情報で更新する。
S233:MAプロトコル制御部40はMAVPN制御部41を起動する。
S234:モバイルIPプロトコル処理部45は、受信メッセージが位置登録要求(Reg. Request)の場合、位置登録応答(Reg. Reply)を送信する。受信メッセージがBUの場合、BAを送信する。

登録要求(BU)、登録応答(BA)の場合:

S235:モバイルIPプロトコル処理部45は受信メッセージがBUであれば、S235へ、BAであればS234へ処理を分岐する。モバイルエージェント(MA)がPCNとして動作している場合は、PCN配下のCN宛てのBUメッセージを全て代理受信する。この仕組みは、例えば特願2000-32372号の方式で実現される。

S236:処理を要求してきたMAがPCNの場合、モバイルIPプロトコル処理部45はBUメッセージに設定されたVPN情報をVPN情報キャッシュに設定もしくは置換する。

【0074】

図33は、図27内に示されるMAVPN制御部41の処理フローの例である。

S240:MAVPN制御部41は、VPNを張るために、トンネル制御部47を起動する。

【0075】

図34及び図35は、図27内に示されるトンネル制御部47の処理フローの例である。

S250:周期位置登録の場合、新しいVPNへ切り替える為にトンネル制御部47はVPN情報インスタンスの情報を元にネットワークカーネル42に設定済みのルートテーブル情報とVPN情報テーブル48の該当する情報を削除する。

S251:トンネル制御部47はVPN情報インスタンスのVPN情報プロファイルに設定されたVPN種別に応じてネットワークカーネル42のルートテーブルに設定する。ルートテーブルの出力デバイスインタフェースはVPN種別がIPinIPなら物理デバイス、IPSecまたはIPSec+UDPならばIPSec仮想デバイスへ出力する。

S252:トンネル制御部47はVPN情報テーブル48にトンネル情報を設定する。

S253:トンネル制御部47は位置登録要求メッセージ(Reg. Request)内の気付けアドレスから、通信事業者または相互接続契約した通信事業者のグローバルアドレス運用によるセキュアなアクセス網(今の場合、CDMA通信システムで構成されている通信事業者のアクセス網はセキュリティが非常に高いものとしている)への通信ならばS255へ、通信事業者または相互接続契約した通信事業者のグローバルアドレス運用による非セキュアなアクセス網(例えば、店舗内のみなどに限定された無線LANなどのホットスポットが考えられる)ならばS256、それ以外ならS254へ処理を分岐させる。アドレスによる判定処理はDNS(Domain Name System)に問い合わせ、ドメイン比較による処理でもよい。

S254:トンネル制御部47は位置登録要求メッセージ(Reg. Request)の送信元アドレスと気付けアドレスを比較し、一致すれば企業網内からのアクセスとしS255、一致しなければプライベートアドレス運用による相互接続契約した通信事業者運用のアクセス網からのアクセスとしS257へ処理を分岐する。アドレスによる判定処理はDNS(Domain Name System)に問い合わせ、ドメイン比較による処理でもよい。

S255:トンネル制御部47はVPN種別にIPinIPを設定する。

S256:トンネル制御部47はVPN種別にIPSecを設定する。

S257:トンネル制御部47はVPN種別にIPSec+UDPを設定する。

S260:トンネル制御部47はVPN種別がIPinIPならば処理を終了し、IPSecならばS262、IPSec、IPSec+UDPならばS261へ処理を分岐させる。

S261:ネットワークカーネル42はVPN情報インスタンスのポート番号を用いてUDPカプセル化を行う。

S 2 6 2 : ネットワークカーネル 4 2 は V P N 情報インスタンスの V P N 情報プロフィール内 S P I を参照して、S P I がユーザ個別であれば S 2 6 3 へ、デフォルト S P I であれば S 2 6 4 へ処理を分岐する。デフォルト S P I は予めモバイルエージェント (M A) 内に初期構成時に設定される、又はモバイルエージェント (M A) のローカルな保守コンソールから設定されているものとする。

S 2 6 3 : ネットワークカーネル 4 2 は I P S e c 情報インスタンスに E S P 識別子を設定する。

S 2 6 4 : ネットワークカーネル 4 2 は I P S e c 情報インスタンスにトンネル識別子を設定する。

【 0 0 7 6 】

図 3 6 は、図 1 における M N 1 6 の機能ブロックの例を示す。

M N というネットワーク装置は、M N プロトコル制御部 5 0、M N V P N 制御部 5 1、ネットワークカーネル 5 2、ネットワークデバイスインタフェース 5 3 から構成される。

【 0 0 7 7 】

M N プロトコル制御部 5 0 は、モバイル I P を制御するモバイル I P プロトコル処理部 5 4 から構成される。M N V P N 制御部 5 1 は、トンネル制御部 5 5 から構成される。トンネル制御部 5 5 は V P N 情報テーブル 5 6 に設定された V P N 種別に応じて送信先の I P アドレスに対してルートテーブル 5 8 の出力デバイスを書き換える。I P i n I P の場合トンネル仮想デバイスに、I P S e c また I P S e c + U D P の場合 I P S e c 仮想デバイスに書き換える。V P N 情報キャッシュ 5 7 (図 2 2) から読み込まれた V P N 情報テーブル 5 6 に V P N 情報を設定する。

【 0 0 7 8 】

ネットワークカーネル 5 2 により仮想デバイスに出力されたパケットは V P N 情報テーブル 5 6 を参照して、暗号化／復号化及びカプセル化／デカプセル化が実行される。V P N 情報テーブル 5 6、ネットワークカーネル 5 2、ネットワークデバイスインタフェース 5 3 は A A A の詳細説明の中で既に述べたので、詳細は省略する。

【 0 0 7 9 】

図 3 7 から図 4 1 は、M N の処理フローである。以下、これらのフローを用いて M N の処理を説明する。

図 3 7 は、M N の全体処理フローの例である。

S 3 0 0 : ネットワークカーネル 5 8 は物理ネットワークインタフェース 5 3 よりパケットを受信すると、既に概略を説明したようにデカプセル化、復号化を行った後、パケットがシグナリングパケットかデータパケットかで切り分ける。シグナリングパケットのであるかいは M N プロトコル制御部 5 0 が指定した I P のポート番号でパケットを受信したかどうかで決定される。シグナリングパケットであれば S 3 0 1、それ以外であれば S 3 0 3 へ処理を分岐する。

S 3 0 1 : M N プロトコル制御部 5 0 はネットワークカーネルからシグナルパケットを受信し、モバイル I P プロトコルの処理を行う。

S 3 0 2 : M N V P N 制御部 5 1 を起動し、V P N 情報の設定を行う。

S 3 0 3 : ネットワークカーネル 5 2 は受信パケットの出力先のインタフェースを、ルーティングテーブルを参照して決定する。出力先が仮想デバイスであればカプセル化や暗号化が行われ、再度ネットワークカーネル 4 2 はカプセル化した宛先でルーティングテーブルを参照し、出力デバイスを決定する。出力先が物理デバイスであれば、そのデバイスへパケットを送信する。

【 0 0 8 0 】

図 3 8 は、図 3 6 内で示される M N プロトコル制御部 5 0 の処理フローの例である。

S 3 1 0 : 受信したパケットの I P のポート番号を調べ、モバイル I P プロトコルであればモバイル I P プロトコル処理部を起動し処理を終了する。

【 0 0 8 1 】

図 3 9 は、図 3 6 内に示されるモバイル I P プロトコル処理部 5 4 の処理フローの例であ

る。

S320: モバイルIPプロトコル処理部54は受信メッセージのタイプを調べ、DHCPならS321へ、位置登録応答メッセージ(Reg. Reply)ならS327へ処理を分岐する。

S321: モバイルIPプロトコル処理部54はDHCPで通知されたアドレスを調べ、MNの気付アドレスに一致するならS323へ、不一致ならS322へ処理を分岐する。

S322: モバイルIPプロトコル処理部54はDHCPACKメッセージから、気付アドレスとなるIPアドレスとネットワークのドメイン名を取得する。

S323: モバイルIPプロトコル処理部54はDHCPで取得したアドレスを調べ、企業網のアドレスと一致した場合は、S325へ、通信事業者または相互接続契約した通信事業者のグローバルアドレスによる運用が行われているアクセス網のアドレスと一致した場合は、S326へ、相互接続契約した通信事業者のローカルアドレスによる運用が行われているアクセス網の場合はS324へ処理を分岐する。アドレスによる判定処理はDNS(Domain Name System)に問い合わせ、ドメイン比較による処理でもよい。

S324: モバイルIPプロトコル処理部54はHAのグローバルなアドレスにUDPトンネル要求ありの位置登録要求メッセージ(Reg. Request)を送出し、処理を終了する。

S325: モバイルIPプロトコル処理部54はHAのプライベートなアドレスに位置登録要求メッセージ(Reg. Request)を送出し、処理を終了する。

S326: モバイルIPプロトコル処理部54はHAのグローバルなアドレスに位置登録要求メッセージ(Reg. Request)を送出し、処理を終了する。

S327: モバイルIPプロトコル処理部54は位置登録応答メッセージ(Reg. Reply)に設定されたVPN情報をVPN情報キャッシュ57に設定する。

S328: モバイルIPプロトコル処理部54はMN VPN制御部51を起動し処理を終了する。

【0082】

図40は、図36内に示されるMN VPN制御部51の処理フローの例である。

S330: MN VPN制御部51はVPNを張るため、トンネル制御部55を起動し処理を終了する。

【0083】

図41は、図36内に示されるトンネル制御部55の処理フローの例である。

S340: 周期位置登録の場合、新しいVPNへ切り替える為にトンネル制御部55はVPN情報インスタンスの情報を元にネットワークカーネルに設定済みのルートテーブル情報とVPN情報テーブル56の該当する情報を削除する。

S341: トンネル制御部55はVPN情報インスタンスのVPN情報プロファイルに設定されたVPN種別に応じて出力デバイスを設定する。VPN種別がIP in IPなら物理デバイス、IPSecまたはIPSec+UDPならばIPSec仮想デバイスへ出力する。

S342: トンネル制御部55はVPN情報インスタンスのVPN情報プロファイルを参照して、IPSec情報テーブルのトンネル情報インスタンスを設定する。

S343: トンネル制御部55はVPN情報インスタンスのVPN種別を参照して、IP in IPであればトンネリング処理を終了し、IPSecであればS345へ処理を分岐し、IPSec+UDPであればS344へ処理を分岐する。

S344: ネットワークカーネル52はVPN情報インスタンスのIPのポート番号を用いてUDPカプセル化を行う。

S345: ネットワークカーネル52はVPN情報インスタンスのVPN情報プロファイル内SPIを参照して、SPIがユーザ個別であればS346へ、デフォルトSPIであればS347へ処理を分岐する。デフォルトSPIは予めMN内に初期構成時に設定されている、又はMNのローカルな保守コンソールから設定されているものとする。

S 3 4 6 : ネットワークカーネル 5 2 は I P S e c 情報インスタンスに E S P 識別子を設定する。

S 3 4 7 : ネットワークカーネル 5 2 は I P S e c 情報インスタンスにトンネル識別子を設定する。

【 0 0 8 4 】

以下、MNがネットワークにアクセスした時にどのようにしてVPNが設定されていくかを幾つかの例を示して説明する。以降の実施形態では、HAを通信事業者網内に設置されたことを想定して説明を行うが、HAを企業網内に設置した場合においても同様である。トンネルを終端するネットワーク装置でのカプセル化、デカプセル化については企業網内同一拠点からのアクセス時におけるVPN設定方式で詳細に述べる。VPN設定方式は、それ以外の実施形態でも動作は同様である為、その他の実施形態では説明を省略する。

・企業網内同一拠点からのアクセス時におけるVPN設定方式

図 4 2 及び図 4 3 は、本発明の実施形態に従った、企業網内で通信する場合を説明する図である。

【 0 0 8 5 】

図 4 2 に示すとおり、企業網拠点 A に存在する MN から企業網の同一拠点内である CN と通信を行った場合の VPN 設定とパケットルーティングについて示す。企業網内のある拠点に存在する MN の位置登録手順における I P i n I P V P N の設定シーケンスを図 4 3 に示す。図 4 3 で示される MN はホームアドレスとして 1 0 . 1 0 . 2 5 5 . 1 が割り振られており、通信事業者網内に設置された HA にはモバイル IP 用の企業網としてプライベートなネットワークである仮想ホームセグメントが設定されている。その仮想ホームセグメントとのゲートウェイアドレスとして 1 0 . 1 0 . 2 5 5 . 1 0 0 のプライベートなアドレスが設定されている。

【 0 0 8 6 】

P C N - H A 間は静的に I P S e c が設定されており、H A と P C N のルーティングテーブルにはルーティング可能なルートが設定されている (1) 。

M N は D H C P サーバに D H C P R E Q U E S T を送信し、D H C P A C K を受信することで、ネットワーク内でルーティング可能な IP アドレス [1 0 . 1 0 . 1 . 1 0 0] とドメイン名 [a s y a . c o m] を取得する (2) 、 (3) 。

【 0 0 8 7 】

送信元アドレスを D H C P で割り振られた企業網のプライベートなアドレス [1 0 . 1 0 . 1 . 1 0 0] を気付かけアドレスとし、送信先アドレスを H A のプライベートなアドレス [1 0 . 1 0 . 2 5 5 . 1 0 0] とする、N A I 拡張と A A A 認証ヘッダを含む位置登録要求メッセージ (R e g . R e q u e s t) を H A 宛に送信する (4) 。

【 0 0 8 8 】

P C N - H A 間は静的に I P S e c による VPN が設定されている為、P C N 装置内にて、送信先アドレスが H A のプライベートなアドレス [1 0 . 1 0 . 2 5 5 . 1 0 0] であるので、ルーティングテーブルを参照し、I P S e c 0 仮想インタフェースへパケットを送出する。I P S e c 0 仮想インタフェースでパケットを受信すると、I P S e c の設定で指定された暗号化アルゴリズムを使用し、受信パケットを暗号化し、P C N のグローバルなアドレスを送信元アドレス [1 0 0 . 1 . 1 . 1 0 0] 、送信先アドレスを H A のグローバルなアドレス [1 0 0 . 1 . 1 . 1] とした IP ヘッダと I P S e c ヘッダを付加した I P S e c カプセル化を行い、ルーティングテーブルを参照し、実インタフェース e t h 1 から H A へパケットが送信される (5) 。

【 0 0 8 9 】

M N からの位置登録要求メッセージ (R e g . R e q u e s t) を受信した H A は、ルーティングテーブルを参照し、パケットの送信先アドレスが H A のグローバルなアドレス [1 0 0 . 1 . 1 . 1] であることから、実インタフェース e t h 0 でパケットを受信する。I P S e c ヘッダを参照し、オリジナルパケットの暗号をデコードする。デコードされたパケットの送信先アドレスが H A のインタフェースアドレスであるプライベートなア

ドレス [10. 10. 255. 100] であるので、パケットを終端し、アプリケーションであるMAプロトコル制御部へ位置登録要求メッセージ (Reg. Request) を渡す。HAは、位置登録要求メッセージ (Reg. Request) の解析を行い、解析結果に従いAAAに認証要求メッセージ (AMR) を送信する (6)。

【0090】

AAAはAMRメッセージに含まれたNAIでVPNデータベースを検索し、このユーザに固有のVPN情報を抽出する。MNの気付けアドレスのネットワークアドレスが企業網ネットワークであることから、VPN種別にIPinIPを設定したVPN情報をサービスプロファイルに設定する。SPC固定部 (図7) にサービスプロファイルを設定した位置登録要求メッセージ (Reg. Request) をホームエージェント登録要求メッセージ (HAR) に設定し、HA宛に送信する (7)。

【0091】

HAはホームエージェント登録要求メッセージ (HAR) で通知されたVPN情報をVPN情報キャッシュに設定し、HAはホームエージェント登録応答メッセージ (HAA) にサービスプロファイルを含んだ位置登録応答 (Reg. Reply) を設定し、AAAへ送信する (8)。

【0092】

AAAはホームエージェント登録応答メッセージ (HAR) で通知された位置AAAはSPC固定部 (図7) にVPN情報を設定したモバイルIPプロトコルの位置登録応答 (Reg. Reply) を含んだホームエージェント登録応答メッセージ (HAA) を受信すると、位置登録応答 (Reg. Reply) に認証子を付加し、HA宛に認証応答 (AMA) を送信する (9)。

【0093】

HAは移動結合テーブルにMNのホームアドレス [10. 10. 255. 1] と気付けアドレス [10. 10. 1. 100] を移動結合テーブルに設定する。IPinIPトンネルの為のVPN情報を設定したサービスプロファイルを設定した位置登録応答 (Reg. Reply) を返し、ルーティングテーブルに、送信先アドレスがMNのホームアドレス [10. 10. 255. 1] とするパケットをMNの気付けアドレス宛 [10. 10. 255. 100] に送信する為のトンネルを設定し、HAからMN方向へのIPinIPVPNを設定する (10)、(11)。

【0094】

MNは位置登録応答 (Reg. Reply) を受信すると、サービスプロファイルに従い、MNからHA方向にIPinIPVPNを設定する。

図44から図46は、企業網内における経路の切り替え方を説明する図である。

【0095】

図44に示すような企業網内のMNと企業網内のCNで通信を行う場合に、CNからMN方向のパケットをHAへは転送せず、企業網内のPCNにてパケットを折り返し、企業網内に閉じた通信を可能とする。このHAからPCNにパケット折り返しを指示し、経路を最適化する為のシーケンスを図45に示す。

【0096】

図45においては、まず、HAからPCNに対し結合要求メッセージ (BU) を送信する (12)。

PCNは通知されたホームアドレス [10. 10. 255. 1] と気付けアドレスリスト [10. 10. 1. 100] を移動結合テーブルに設定する。MNのホームアドレスを送信先アドレスとするパケットをMNの気付けアドレス宛に送信するようルーティングテーブルにトンネルを設定する。PCNは結合応答メッセージ (BA) を返す (13)。

【0097】

経路最適化後、CNからMN方向へのデータパケットは、CNからPCNへルーティングされ、PCNで折り返され、MNへ送信される。経路最適化後のデータパケットのルーティングを図46に示す。

【0098】

MNからCN方向へのパケットは送信元アドレスをMNのホームアドレス[10. 10. 255. 1]とし、送信先アドレスをCNのプライベートなアドレス[10. 10. 2. 100]とし、PCNを経由し、CNへ転送される(14)。

【0099】

CNからMN方向へのパケットは送信元アドレスをCNのプライベートなアドレス[10. 10. 1. 2]、送信先アドレスをMNのホームアドレス[10. 10. 255. 1]としPCNへと転送される。PCNにて移動結合テーブルを参照し、送信元アドレスをCNのプライベートなアドレス[10. 10. 2. 1]、送信先アドレスをMNの気付けアドレス[10. 10. 1. 100]とするモバイルIPプロトコルによるカプセル化が行われ、MNへと転送される(15)。

・企業網内他拠点からのアクセス時における拠点間通信に既存設備を流用したVPN設定方式

図47及び図48は、同一管理ドメイン内の拠点間通信について説明する図である。

【0100】

図47に示すような企業網間通信には企業網拠点AのGWと企業網拠点BのGW間に張られた既存VPNを使用し、企業網拠点A内のPCNと通信事業者網に設置したHA間にのみに新たにVPNを設定したネットワーク構成で、企業網内拠点Aに存在するMNから企業網の異なる拠点Bに存在するCNと通信を行った場合のVPN設定とパケットルーティングについて示す。企業網内拠点Aに存在するMNの位置登録手順におけるIPinIPVPN設定シーケンスを図48に示す。

【0101】

図48においては、MNはDHCPを利用して、IPアドレス[10. 10. 1. 100]とドメイン名[asya.com]を取得する(1)、(2)。

送信元アドレスをDHCPで割り振られた企業網のプライベートなアドレス[10. 10. 1. 100]、送信先アドレスをHAのグローバルなアドレス[100. 1. 1. 1]とする、NAI拡張とAAA認証ヘッダを含む位置登録要求メッセージ(Reg. Request)をHA宛に送信する(3)。

【0102】

企業網GW-HA間は静的にIPSecによるVPNが設定されている為、企業網GWにて送信元アドレスを企業網GWのグローバルなアドレス[100. 1. 1. 100]、送信先アドレスをHAのグローバルなアドレス[100. 1. 1. 1]としたIPSecカプセル化を行い、HAへ転送する(4)。

【0103】

MNからの位置登録要求メッセージ(Reg. Request)を受信したHAはIPSecデカプセル化を行い、AAAに認証要求メッセージ(AMR)を送信する(5)。

【0104】

AAAはAMRメッセージに含まれたNAIでVPNデータベースを検索し、このユーザに固有のVPN情報を抽出する。MNの気付けアドレスのネットワークアドレスが企業網ネットワークであることから、VPN種別にIPinIPを設定したVPN情報をサービスプロファイルに設定する。SPC固定部(図7)にサービスプロファイルを設定した位置登録要求メッセージ(Reg. Request)をホームエージェント登録要求メッセージ(HAR)に設定し、HA宛に送信する(6)。

【0105】

HAはホームエージェント登録要求メッセージ(HAR)で通知されたVPN情報をVPN情報キャッシュに設定し、HAはホームエージェント登録応答メッセージ(HAA)にサービスプロファイルを含んだ位置登録応答(Reg. Reply)を設定し、AAAへ送信する(7)。

【0106】

AAAはSPC固定部(図7)にVPN情報を設定したモバイルIPプロトコルの位置登

録応答 (Reg. Reply) を含んだホームエージェント登録応答メッセージ (HAA) を受信すると、登録応答 (Reg. Reply) に認証子を付加し、HA宛に認証応答 (AMA) を送信する (8)。

【0107】

HAはVPN種別にIPinIPを設定した位置登録応答 (Reg. Reply) を返し、HAからMN方向へのIPinIPVPNを設定する (9)、(10)。

MNは位置登録応答 (Reg. Reply) を受信すると、サービスプロファイルに従い、MNからHA方向にIPinIPVPNを設定する。

【0108】

図49から図51は、企業網内における経路切り替え方を説明する図である。

図49に示すような企業網内のMNと企業網内のCNで通信を行う場合に、CNからMN方向のパケットをHAへは転送せず、企業網GW間に設定されているVPNを通り、企業網内のPCNにてパケットを折り返し、企業網内に閉じた通信を可能とする。このHAからPCNにパケット折り返しを指示し、経路を最適化する為のシーケンスを図50に示す。

【0109】

図50においては、まず、HAからPCNに対し結合要求メッセージ (BU) を送信する (11)。通信事業者網と企業網GW間はIPSecによるトンネリングによりメッセージが転送される。

【0110】

PCNは通知されたホームアドレスと気付けアドレスリストを移動結合テーブルに設定する。MNのホームアドレスを送信先アドレスとするパケットをMNの気付けアドレス宛に送信するようルーティングテーブルにトンネルを設定する。そして、PCNは結合応答メッセージ (BA) をHAに返す (12)。

【0111】

経路最適化後、CNからMN方向へのデータパケットは、CNからPCNへルーティングされ、PCNで折り返され、MNへ送信される。経路最適化後のデータパケットのルーティングを図51に示す。

【0112】

図51においては、MNからCN方向へのパケットは送信元アドレスをMNのホームアドレス [10. 10. 255. 1] とし、送信先アドレスをCNのプライベートなアドレス [10. 10. 2. 100] とし、企業網既存VPNを経由し、CNへ転送される (13)。

【0113】

CNからMN方向へのパケットは送信元アドレスをCNのプライベートなアドレス [10. 10. 2. 100]、送信先アドレスをMNのホームアドレス [10. 10. 255. 1] としPCN送信する。PCNにて移動結合テーブルを参照し、送信元アドレスをCNのプライベートなアドレス [10. 10. 2. 100]、送信先アドレスをMNの気付けアドレス [10. 10. 1. 100] とするモバイルIPプロトコルによるカプセル化が行われ、MNへと転送される (14)。

・企業網内他拠点からのアクセス時における拠点間通信に拠点毎VPN設定方式図52及び図53は、同一管理ドメイン内の拠点間通信を説明する図である。

【0114】

図52に示すような企業網間通信には企業網拠点AのGWと企業網拠点BのGW間に張られた既存VPNを使用し、HAとの通信の為に、新たに企業網拠点A内にPCN1と企業網拠点B内にPCN2を設置し、PCN1、PCN2とHA間にVPNを設定したネットワークにおいて、企業網内拠点Aに存在するMNからの企業網内拠点Bに存在するCNと通信を行った場合のIPinIPVPN設定とパケットルーティングについて示す。企業網Aのある拠点に存在するMNの位置登録手順におけるIPinIPVPN設定シーケンスを図53に示す。

【0115】

図53においては、まず、DHCPを利用しIPアドレス[10.10.1.100]とドメイン名[asya.com]を取得する(1)、(2)。

送信元アドレスにDHCPで割り振られた企業網のプライベートなアドレス[10.10.1.100]、送信先アドレスにHAのグローバルなアドレス[100.1.1.1]を設定し、NAI拡張とAAA認証ヘッダを含む位置登録要求メッセージ(Reg. Request)をHA宛に送信する(3)。

【0116】

PCN1-HA間は静的にIPSecによるVPNが設定されている為、PCN2にて送信元アドレスをPCN2のグローバルなアドレス[100.1.1.100]、送信先アドレスをHAのグローバルなアドレス[100.1.1.1]としたIPSecカプセル化を行い、HAへ転送する(4)。

【0117】

MNからの位置登録要求メッセージ(Reg. Request)を受信したHAはIPSecデカプセル化を行い、AAAに認証要求メッセージ(AMR)を送信する(5)。

【0118】

AAAはAMRメッセージに含まれたNAIでVPNデータベースを検索し、このユーザに固有のVPN情報を抽出する。MNの気付けアドレスのネットワークアドレスが企業網ネットワークであることから、VPN種別にIPinIPを設定したVPN情報をサービスプロファイルに設定する。SPC固定部(図7)にサービスプロファイルを設定した位置登録要求メッセージ(Reg. Request)をホームエージェント登録要求メッセージ(HAR)に設定し、HA宛に送信する(6)。

【0119】

HAはホームエージェント登録要求メッセージ(HAR)で通知されたVPN情報をVPN情報キャッシュに設定し、HAはホームエージェント登録応答メッセージ(HAA)にサービスプロファイルを含んだ位置登録応答(Reg. Reply)を設定し、AAAへ送信する(7)。

【0120】

AAAはSPC固定部(図7)にVPN情報を設定したモバイルIPプロトコルの位置登録応答(Reg. Reply)を含んだホームエージェント登録応答メッセージ(HAA)を受信すると、登録応答(Reg. Reply)に認証子を付加し、HA宛に認証応答(AMA)を送信する(8)。

【0121】

HAはVPN種別にIPinIPを設定した位置登録応答(Reg. Reply)を返し、HAからMN方向へのIPinIPVPNを設定する(9)、(10)。

MNは位置登録応答(Reg. Reply)を受信すると、サービスプロファイルに従い、MNからHA方向にIPinIPVPNを設定する。

【0122】

図54から図56は、PCN1-PCN2間の経路最適化方式を説明する図である。

図54に示すような企業網拠点A内のMNと企業網拠点B内のCNで通信を行う場合に、CNからMN方向のパケットをHAへは転送せず、企業網GW間に設定されたVPNを通り、企業網A内のPCN1にてパケットを折り返し、企業網内に閉じた通信を可能とする。このHAからPCNにパケット折り返しを指示し、経路を最適化する為のシーケンスを図55に示す。

【0123】

図55においては、HAからCN側PCN1に対し、結合要求メッセージ(BU)を送信する(11)。

PCN1は通知されたホームアドレスと気付けアドレスリストを移動結合テーブルに設定する。送信先アドレスがMNのホームアドレスとなるパケットをPCN2へ送信するようルーティングテーブルにトンネルを設定する。結合応答メッセージ(BA)を送信する(

12)。

【0124】

経路最適化後、CNからMN方向へのデータパケットは、CNから企業網のGW間に設定されたVPNを使用し、PCN1からPCN2へルーティングされ、MNへ送信される。経路最適化後のデータパケットのルーティングを図56に示す。

【0125】

MNからCN方向へのパケットは送信元アドレスをMNのホームアドレス[10.10.255.1]とし、送信先アドレスをCNのプライベートなアドレス[10.10.2.100]とし、PCN1を経由し、CNへ転送される(13)。

【0126】

CNからMN方向へのパケットは送信元アドレスをCNのプライベートなアドレス[10.10.2.100]、送信先アドレスをMNのホームアドレス[10.10.255.1]としPCN2に送信する。PCN2にて結合テーブルを参照し、送信元アドレスをCNのプライベートなアドレス[10.10.2.100]、送信先アドレスをMNの気付けアドレス[10.10.1.100]とするモバイルIPプロトコルによるカプセル化が行われ、MNへと転送される(14)。

・通信事業者のセキュアなアクセス網(例CDMA通信網)からのアクセス時におけるVPN設定方式

図57から図59は、移動通信事業者を介した通信について説明する図である。

【0127】

図57に示すようなMNは通信事業者によってセキュリティが保証された通信事業者網に存在し、企業網に設置されたPCNと通信事業者網に設置されたHA間にIPSecによるVPNが設定されたネットワークにおいて、企業網内のCNとセキュリティが保証された通信事業者網である外部ネットワークに存在するMNと通信を行った場合のVPN設定とパケットルーティングについて示す。セキュリティが保証された通信事業者網である外部ネットワークに存在するMNの位置登録手順におけるIPinIP VPN設定シーケンスを図58に示す。

【0128】

図58においては、MNはDHCPを利用しIPアドレス[200.2.1.100]とドメイン名[docomo.com]を取得する(1)、(2)。

送信元アドレスにDHCPで割り振られた通信事業者網のアドレス[200.2.1.100]、送信先アドレスにHAのグローバルなアドレス[200.1.1.101]を設定し、NAI拡張とAAA認証ヘッダを含む位置登録要求メッセージ(Reg. Request)をHA宛に送信する(3)。

【0129】

MNからの位置登録要求メッセージ(Reg. Request)を受信したHAはAAAに認証要求メッセージ(AMR)を送信する(4)。

AAAはAMRメッセージに含まれたNAIでVPNデータベースを検索し、このユーザに固有のVPN情報を抽出する。MNの気付けアドレスのネットワークアドレスがセキュアな通信事業者網であることから、VPN種別にIPinIPを設定したVPN情報をサービスプロファイルに設定する。SPC固定部(図7)にサービスプロファイルを設定した位置登録要求メッセージ(Reg. Request)をホームエージェント登録要求メッセージ(HAR)に設定し、HA宛に送信する(5)。

【0130】

HAはホームエージェント登録要求メッセージ(HAR)で通知されたVPN情報をVPN情報キャッシュに設定し、HAはホームエージェント登録応答メッセージ(HAA)にサービスプロファイルを含んだ位置登録応答(Reg. Reply)を設定し、AAAへ送信する(6)。

【0131】

AAAはSPC固定部(図7)にVPN情報を設定したモバイルIPプロトコルの位置登

録応答 (Reg. Reply) を含んだホームエージェント登録応答メッセージ (HAA) を受信すると、登録応答 (Reg. Reply) に認証子を付加し、HA宛に認証応答 (AMA) を送信する (7)。

【0132】

HAはVPN種別にIPinIPを設定した位置登録応答 (Reg. Reply) を返し、HAからMN方向へのIPinIPVPNを設定する (8)。

MNは位置登録応答 (Reg. Reply) を受信すると、サービスプロファイルに従い、MNからHA方向にIPinIPVPNを設定する。

上記で設定されたVPNを使用し、HAを経由しMN-CN間の通信が行われる。データパケット交換シーケンスを図59に示す。図59は通信事業者網からの接続シーケンスを示している。

【0133】

図59においては、MNからCN方向へのパケットはMNのco-locatedモードにより外部IPヘッダの送信元アドレスに通信事業者網で割り振られたアドレス [200. 2. 1. 100]、送信先アドレスにHAアドレス [100. 1. 1. 1]、内部IPヘッダの送信元アドレスにMNのホームアドレス [10. 10. 255. 1]、送信先アドレスをCNのプライベートなアドレス [10. 10. 2. 100] としたパケットが生成され、HAへ送信される。PCN-HA間は静的にIPSecによるVPNが設定されている為、HAにて送信元アドレスをHAのグローバルなアドレス [100. 1. 1. 1]、送信先アドレスをPCNのグローバルなアドレス [100. 1. 1. 100] としたIPSecカプセル化を行い、PCNへ転送される。PCNにてIPSecデカプセル化を行い、CNへ送信する (9)。

【0134】

CNからMN方向へのパケットは送信元アドレスをCNのプライベートなアドレス [10. 10. 2. 100]、送信先アドレスをMNのホームアドレス [10. 10. 255. 1] としPCNへ送信される。PCNにて送信元アドレスをPCNグローバルなアドレス [100. 1. 1. 100]、送信先アドレスをHAのグローバルなアドレス [100. 1. 1. 1] としたIPSecカプセル化を行い、HAへ送信する。HAではIPSecデカプセル化を行い、モバイルIPプロトコルによるカプセル化を行い、MNへ送信する (10)。

・通信事業者の非セキュアなアクセス網 (例ホットスポット) からのアクセス時におけるVPN設定方式

図60から図62は、移動通信事業者網直結ホットスポットからの通信動作を説明する図である。

【0135】

図60に示すようなMNは通信事業者によってセキュリティが保証されていないホットスポットに存在し、企業網に設置されたPCNと通信事業者網に設置されたHA間にIPSecによるVPNが設定されたネットワークにおいて、企業網内のCNとセキュリティが保証されていないホットスポット網である外部ネットワークに存在するMNと通信を行った場合のVPN設定とパケットルーティングについて示す。セキュリティが保証されていないホットスポットに存在するMNの位置登録手順におけるIPSec VPN設定シーケンスを図61に示す。

【0136】

図61においては、MNはDHCPを利用しIPアドレス [200. 20. 1. 100] とドメイン名 [docomo. com] を取得する (1)、(2)。

送信元アドレスにDHCPで割り振られた通信事業者網のアドレス [200. 20. 1. 100]、送信先アドレスにHAのグローバルなアドレス [100. 1. 1. 1] を設定し、NAI拡張とAAA認証ヘッダを含む位置登録要求メッセージ (Reg. Request) をHA宛に送信する (3)。

【0137】

MNからの位置登録要求メッセージ (Reg. Request) を受信したHAはAAAに認証要求メッセージ (AMR) を送信する (4)。

AAAはAMRメッセージに含まれたNAIでVPNデータベースを検索し、このユーザに固有のVPN情報を抽出する。MNの気付けアドレスのネットワークアドレスが非セキュアな通信事業者網であることから、VPN種別にIPSecを設定したVPN情報をサービスプロファイルに設定する。SPC固定部 (図7) にサービスプロファイルを設定した位置登録要求メッセージ (Reg. Request) をホームエージェント登録要求メッセージ (HAR) に設定し、HA宛に送信する (5)。

【0138】

HAはホームエージェント登録要求メッセージ (HAR) で通知されたVPN情報をVPN情報キャッシュに設定し、HAはホームエージェント登録応答メッセージ (HAA) にサービスプロファイルを含んだ位置登録応答 (Reg. Reply) を設定し、AAAへ送信する (6)。

【0139】

AAAはSPC固定部 (図7) にVPN情報を設定したモバイルIPプロトコルの位置登録応答 (Reg. Reply) を含んだホームエージェント登録応答メッセージ (HAA) を受信すると、登録応答 (Reg. Reply) に認証子を付加し、HA宛に認証応答 (AMA) を送信する (7)。

【0140】

HAはVPN種別にIPSecを設定した位置登録応答 (Reg. Reply) を返し、HAからMN方向へのIPSecVPNを設定する (8)。

MNは位置登録応答 (Reg. Reply) を受信すると、サービスプロファイルに従い、MNからHA方向にIPSecVPNを設定する。

【0141】

上記で設定されたVPNを使用し、HAを経由しMN-CN間の通信が行われる。データパケット交換シーケンスを図62に示す。

MNからCN方向へのパケットはMNのco-locatedモードにより外部IPヘッダの送信元アドレスに通信事業者網で割り振られたアドレス [200. 20. 1. 100]、送信先アドレスにHAのグローバルなアドレス [100. 1. 1. 1]、内部IPヘッダの送信元アドレスにMNのホームアドレス [10. 10. 255. 1]、送信先アドレスをCNのプライベートなアドレス [10. 10. 2. 100] としたパケットが生成され、HAへ送信される。PCN-HA間は静的にIPSecによるVPNが設定されている為、HAにて送信元アドレスをHAのグローバルなアドレス [100. 1. 1. 1]、送信先アドレスをPCNのグローバルなアドレス [100. 1. 1. 100] としたIPSecカプセル化を行い、PCNへ転送される。PCNにてIPSecデカプセル化を行い、CNへ送信する (9)。

【0142】

CNからMN方向へのパケットは送信元アドレスをCNのプライベートなアドレス [10. 10. 2. 100]、送信先アドレスをMNのホームアドレス [10. 10. 255. 1] としPCNへ送信される。PCNにて送信元アドレスをPCNグローバルなアドレス [100. 1. 1. 100]、送信先アドレスをHAのグローバルなアドレス [100. 1. 1. 1] としたIPSecカプセル化を行い、HAへ送信する。HAではIPSecデカプセル化を行い、モバイルIPプロトコルによるカプセル化を行い、MNへ送信する (10)。

・通信事業者とローミング契約した他の通信事業者のアクセス網からのアクセス時におけるVPN設定方式

図63から図65は、ローミング提携先からの通信の動作を説明する図である。

【0143】

図63に示すようなMNは通信事業者とローミング契約した他の通信事業者のアクセス網に存在し、企業網に設置されたPCNと通信事業者網に設置されたHA間にIPSecに

よるVPNが設定されたネットワークにおいて、企業網内のCNとローミング契約した他の通信事業者のアクセス網である外部ネットワークに存在するMNと通信を行った場合のVPN設定とパケットルーティングについて示す。通信事業者とローミング契約した他の通信事業者のアクセス網に存在するMNの位置登録手順におけるIPSec+UDP VPN設定シーケンスを図64に示す。

【0144】

図64においては、MNはDHCPを利用しIPアドレス[10.20.1.100]とドメイン名[unknown.com]を取得する(1)、(2)。

送信元アドレスにDHCPで割り振られたローミング先の通信事業者網で割り振られたアドレス[10.20.1.100]、送信先アドレスにHAのグローバルなアドレス[100.1.1.1]を設定し、NAI拡張とAAA認証ヘッダを含む位置登録要求メッセージ(Reg. Request)をHA宛に送信する(3)。

【0145】

MNからの位置登録要求メッセージ(Reg. Request)を受信したHAはAAAに認証要求メッセージ(AMR)を送信する(4)。

AAAはAMRメッセージに含まれたNAIでVPNデータベースを検索し、このユーザに固有のVPN情報を抽出する。MNの気付けアドレスのネットワークアドレスが企業網、セキュアな通信事業者網、非セキュアな通信事業者網でないので、ローミング契約した他の通信事業者のアクセス網と判断し、VPN種別にIPSec+UDPを設定したVPN情報をサービスプロファイルに設定する。SPC固定部(図7)にサービスプロファイルを設定した位置登録要求メッセージ(Reg. Request)をホームエージェント登録要求メッセージ(HAR)に設定し、HA宛に送信する(5)。

【0146】

HAはホームエージェント登録要求メッセージ(HAR)で通知されたVPN情報をVPN情報キャッシュに設定し、HAはホームエージェント登録応答メッセージ(HAA)にサービスプロファイルを含んだ位置登録応答(Reg. Reply)を設定し、AAAへ送信する(6)。

【0147】

AAAはSPC固定部(図7)にVPN情報を設定したモバイルIPプロトコルの位置登録応答(Reg. Reply)を含んだホームエージェント登録応答メッセージ(HAA)を受信すると、登録応答(Reg. Reply)に認証子を付加し、HA宛に認証応答(AMA)を送信する(7)。

【0148】

HAはVPN種別にIPSec+UDPを設定した位置登録応答(Reg. Reply)を返し、HAからMN方向へのIPSec+UDPVPNを設定する(8)。MNは位置登録応答(Reg. Reply)を受信すると、サービスプロファイルに従い、MNからHA方向にIPSec+UDPVPNを設定する。

【0149】

上記で設定されたVPNを使用し、MN-CN間の通信が行われる。データパケット交換シーケンスを図65に示す。

MNからCN方向へのパケットはMNのco-locatedモードにより外部IPヘッダの送信元アドレスに通信事業者網で割り振られたアドレス[10.20.1.100]、送信先アドレスにHAのグローバルなアドレス[100.1.1.1]、内部IPヘッダの送信元アドレスにMNのホームアドレス[10.10.255.1]、送信先アドレスをCNのプライベートなアドレス[10.10.2.100]としたパケットが生成され、HAへ送信される。GWのNAT/NAPT機能により送信元アドレスをGWグローバルなアドレス[100.10.1.100]に書き換えられ、HAへ転送される。PCN-HA間は静的にIPSecによるVPNが設定されている為、HAにて送信元アドレスをHAのグローバルなアドレス[100.1.1.1]、送信先アドレスをPCNのグローバルなアドレス[100.1.1.100]としたIPSec+UDPカプセル化を

行い、PCNへ転送される。PCNにてIPSec+UDPデカプセル化を行い、CNへ送信する(9)。

【0150】

CNからMN方向へのパケットは送信元アドレスをCNのプライベートなアドレス[10.10.2.100]、送信先アドレスをMNのホームアドレス[10.10.255.1]としHAへ送信される。PCNにて送信元アドレスをPCNグローバルなアドレス[100.1.1.100]、送信先アドレスをHAのグローバルなアドレス[100.1.1.1]としたIPSecカプセル化を行い、HAへ送信する。HAではIPSec+UDPデカプセル化を行い、モバイルIPプロトコルによるカプセル化を行い、MNへ送信する。GWのNAT/NAPT機能により送信先アドレスをGWのプライベートなアドレス[10.10.1.100]に書き換えられ、MNへ転送される(10)。

・外部ネットワークからの外部ネットワークへの通信

図66は、企業網内プロキシ経由によるインターネット接続の場合の動作を説明する図である。

【0151】

この実施形態は、外部ネットワークと存在するMNが企業網外のネットワークと通信したパケットルーティングについて示す。外部ネットワーク間のパケット経路図を図66に示す。

【0152】

MNは企業網のGWをプロキシアドレスとし、外部ネットワークに送信する。外部ネットワークからのパケットは企業網のGWを経由し、MNへ送信される。

・通信事業者のセキュアなアクセス網(例FOMA、CDMA)から企業網アクセス時の経路最適化

図67から図69は、移動通信業者網を介した通信の動作を説明する図である。

【0153】

図67において、企業網のPCNと通信事業者網に設定されたHA間にIPSec VPNが設定され、通信事業者コア網に接続されたアクセス網が通信事業者のセキュアなアクセス網(例CDMA)の場合、通信事業者のセキュアなアクセス網のMNから企業網内のCNへ通信する場合に、EaseNet(特願2000-50220)の経路最適化の仕組みを応用して、HAを経由せずにMN-PCN間で直接通信するIPSec VPN設定方法を図68に示す。

【0154】

企業は、IPSecで通信事業者のセキュアなアクセス網(例えばCDMA)をアクセス可能な拠点を、サービスプロファイルとして登録する(1)。

MNが通信事業者のセキュアなアクセス網(例CDMA)に接続された場合、EaseNetは、認証時に、あらかじめ設定されたサービスプロファイルに基づき、VPN情報をHAにダウンロードする。

【0155】

MNへは位置登録応答メッセージを用いて指定された全ての拠点へのVPN情報を配布する(2)、(3)。

HAは、結合更新メッセージを用いて、指定されたそれぞれの拠点のPCNへVPN情報を配布する(4)。

【0156】

配布されたVPN情報により、PCNとMNは直接相手ノードへIPSec VPNを設定する。これによりMNと指定された企業拠点間の通信は、HAを介することなく行うことが可能となる。

【0157】

MNが移動した場合は、認証時と同様な手順でVPNが再設定される。

・通信事業者の非セキュアなアクセス網(例ホットスポット)から企業網アクセス時の経路最適化

図70から図72は、移動通信事業者網直結ホットスポットからの通信の動作を説明する図である。

【0158】

図70において、企業網のPCNと通信事業者網に設定されたHA間にIPSec VPNが設定され、通信事業者コア網に接続されたアクセス網が通信事業者の非セキュアなアクセス網（例ホットスポット）の場合、通信事業者のセキュアなアクセス網のMNから企業網内のCNへ通信する場合に、EaseNet（特願2000-50220）の経路最適化の仕組みを応用して、HAを経由せずにMN-PCN間で直接通信するIPSec VPN設定方法を図71に示す。

【0159】

企業は、IPSecで通信事業者の非セキュアなアクセス網（例ホットスポット）をアクセス可能な拠点を、サービスプロファイルとして登録する（1）。

MNが通信事業者の非セキュアなアクセス網（例ホットスポット）に接続された場合、EaseNetは、認証時に、あらかじめ設定されたサービスプロファイルに基づき、VPN情報をHAにダウンロードする。

【0160】

MNへは位置登録応答メッセージを用いて指定された全ての拠点へのVPN情報を配布する（2）、（3）。

HAは、結合更新メッセージを用いて、指定されたそれぞれの拠点のPCNへVPN情報を配布する（4）。

【0161】

配布されたVPN情報により、PCNとMNは直接相手ノードへIPSec VPNを設定する。これによりMNと指定された企業拠点間の通信は、HAを介することなく行うことが可能となる。

【0162】

MNが移動した場合は、認証時と同様な手順でVPNが再設定される。

・通信事業者とローミング契約した他の通信事業者のアクセス網から企業網アクセス時の経路最適化

図73から図75は、ローミング提携先からの通信の動作を説明する図である。

【0163】

図73において、企業網のPCNと通信事業者網に設定されたHA間にIPSec VPNが設定され、通信事業者コア網に接続されたアクセス網が通信事業者とローミング契約した他の通信事業者のアクセス網の場合、通信事業者のセキュアなアクセス網のMNから企業網内のCNへ通信する場合に、EaseNet（特願2000-50220）の経路最適化の仕組みを応用して、HAを経由せずにMN-PCN間で直接通信するIPSec + UDP VPN設定方法を図74に示す。

【0164】

企業は、IPSec + UDPで通信事業者とローミング契約した他の通信事業者のアクセス網をアクセス可能な拠点とし、サービスプロファイルとして登録する。

【0165】

MNが通信事業者とローミング契約した他の通信事業者のアクセス網に接続された場合、EaseNetは、認証時に、あらかじめ設定されたサービスプロファイルに基づき、VPN情報をHAにダウンロードする。

【0166】

MNへは位置登録応答メッセージを用いて指定された全ての拠点へのVPN情報を配布する（1）、（2）、（3）。

HAは、結合更新メッセージを用いて、指定されたそれぞれの拠点のPCNへVPN情報を配布する（4）。

【0167】

配布されたVPN情報により、PCNとMNは直接相手ノードへIPSec + UDP V

P Nを設定する。これによりM Nと指定された企業拠点間の通信は、H Aを介することなく行うことが可能となる。

【0168】

M Nが移動した場合は、認証時と同様な手順でV P Nが再設定される。

(付記1) プライベートなネットワークである第1のネットワーク内で使用される第1のアドレスを用いて、第2のアドレスを用いて通信を制御する、第1のネットワークに接続された、第2のネットワークを介した通信を行う仮想閉域網システムであって、該第1のアドレスを固定的に保持して通信を行う、移動可能な第1の手段と、該第1の手段の第1のアドレスと、第2のネットワークを介した通信を行うための第2のアドレスとの対応関係を取得し、該第1の手段が移動しても通信

可能なセッションの確立を行う手順の中で、該第1の手段の認証を行い、該第2のネットワークを介して、第1のネットワークにアクセスする通信装置との間に仮想閉域網を形成する第2の手段と、

を備えることを特徴とする仮想閉域網システム。

【0169】

(付記2) 前記第1の手段が、該第1のネットワークに接続した端末と通信を行う場合に、該第1の手段と該端末との通信経路を最適化する手段を更に備えることを特徴とする付記1に記載の仮想閉域網システム。

【0170】

(付記3) 前記第2の手段と、前記第1のネットワーク間には、予め仮想閉域網が設定されていることを特徴とする付記1に記載の仮想閉域網システム。

(付記4) 前記移動通信可能なプロトコルは、モバイルIPであることを特徴とする付記1に記載の仮想閉域網システム。

【0171】

(付記5) 前記第2の手段は、前記第1の手段との間のモバイルIPのトンネル設定手順において、該第1の手段に仮想閉域網に関する情報を通知し、該第1の手段と該第2の手段間に仮想閉域網を設定することを特徴とする付記4に記載の仮想閉域網システム。

【0172】

(付記6) 前記モバイルIPと仮想閉域網の設定において、前記第1の手段のc o o - l o c a t e dモードを利用することを特徴とする付記5に記載の仮想閉域網システム。

【0173】

(付記7) 前記第2のネットワークは、公共ネットワークと、通信事業者の有する移動体通信網とからなり、前記第1の手段がアクセスする該移動体通信網がセキュアなアクセス網である場合には、前記第2の手段と該第1の手段との間にI P i n I Pのトンネルを設定することを特徴とする付記6に記載の仮想閉域網システム。

【0174】

(付記8) 前記第2のネットワークは、公共ネットワークと、通信事業者の有する移動体通信網とからなり、前記第1の手段がアクセスする該移動体通信網が非セキュアなアクセス網である場合には、前記第2の手段と該第1の手段との間にI P S e cのトンネルを設定することを特徴とする付記6に記載の仮想閉域網システム。

【0175】

(付記9) 前記第2のネットワークは、公共ネットワークと、第1の通信事業者の有する第1の移動体通信網と、第2の通信事業者の有する第2の移動体通信網とからなり、前記第1の手段が該第1の移動体通信網から第2の移動体通信網と公共ネットワークを介して前記第1のネットワークにアクセスする場合、前記第2の手段と該第1の手段との間にI P S e c + U D Pのトンネルを設定することを特徴とする付記6に記載の仮想閉域網システム。

【0176】

(付記10) 前記第2の手段と前記第1のネットワークの間には、固定的な仮想閉域網を予め設定しておくことを特徴とする付記1に記載の仮想閉域網システム。

【0177】

(付記11) モバイルIPに従って移動端末とプライベートネットワークに接続された端末の通信を可能にするホームエージェントであって、
該移動端末と該ホームエージェントの間に仮想閉域網を設定する手段と、
該移動端末のアクセス認証を行う手段と、
該移動端末に、該認証手段から得られた該仮想閉域網に関する情報を通知する手段と、
を備えることを特徴とするホームエージェント。

【0178】

(付記12) 移動端末とプライベートネットワークに接続された端末の通信を可能にするルータであって、
該移動端末から送られてくる位置登録要求の気付けアドレスまたはドメインを検出する手段と、
検出した該気付けアドレスまたは該ドメインが通信の秘匿性を確保可能な網を示している場合には、該移動端末と該ルータとの間を秘匿性の低い通信プロトコルで、該気付けアドレスが通信の秘匿性を十分保証しきれない網を示している場合には、該移動端末と該ルータとの間を秘匿性の高い通信プロトコルで、該ルータを経由して該移動端末と該端末との通信を行わせる通信制御手段と、
を備えることを特徴とするルータ。

【0179】

(付記13) 移動端末とプライベートネットワークに接続された端末の通信を可能にするルータであって、
該移動端末から送られてくる位置登録要求の気付けアドレスと送信元アドレスを比較する手段と、
該気付けアドレスが所定の通信事業者を示していない場合であって、該気付けアドレスが該送信元アドレスと一致する場合には、該移動端末と該ルータとの間を秘匿性の低い通信プロトコルで、該気付けアドレスが該送信元アドレスと一致しない場合には、該移動端末と該ルータとの間を秘匿性の高い通信プロトコルで、該ルータを経由して該移動端末と該端末との通信を行わせる通信制御手段と、
を備えることを特徴とするルータ。

【0180】

(付記14) 該移動端末と該ルータとの間を秘匿性の高い通信プロトコルはIPSec+UDPのトンネルであることを特徴とする付記13に記載のルータ。

【0181】

(付記15) プライベートネットワークに接続された端末との通信を可能にする移動端末であって、
該移動端末が現在自身の属する網の情報を取得する取得手段と、
取得した該網の情報がプライベートネットワークであることを示す場合には、該移動端末の位置を管理するルータのプライベートなアドレスに位置登録要求メッセージを送出し、
該網が所定の通信事業者網であることを示す場合には、該ルータのグローバルなアドレスに位置登録要求メッセージを送出し、それ以外の場合には、該ルータのグローバルなアドレスに、秘匿性の高い通信経路の設定要求を含む位置登録要求メッセージを送出するように制御する制御手段と、
を備えることを特徴とする移動端末。

【0182】

(付記16) 該移動端末と該ルータとの間を秘匿性の高い通信プロトコルはIPSec+UDPのトンネルであることを特徴とする付記15に記載のルータ。

【0183】

(付記17) 移動端末とプライベートネットワークに接続された端末の通信を可能にするシステムにおける移動端末であって、
モバイルIPの通信用トンネルを設定する手段と、
該モバイルIPの通信用トンネルの設定手順において、該プライベートネットワークの通

信用トンネルを設定する手段とを備え、

該移動端末は、モバイルIPの通信用トンネルとプライベートネットワークの通信用トンネルを兼用した1つの通信用トンネルを使って通信を行うことを特徴とする移動端末。

【0184】

(付記18) プライベートなネットワークである第1のネットワーク内で使用される第1のアドレスを用いて、第2のアドレスを用いて通信を制御する、第1のネットワークに接続された、第2のネットワークを介した通信を行う仮想閉域網システムにおける通信制御方法であって、

該第1のアドレスを固定的に保持して通信を行う、移動可能な移動端末を設けるステップと、

該移動端末の第1のアドレスと、第2のネットワークを介した通信を行うための第2のアドレスとの対応関係を取得し、該移動端末が移動しても通信可能なセッションの確立を行う手順の中で、該移動端末の認証を行い、該第2のネットワークを介して、第1のネットワークにアクセスする通信装置との間に仮想閉域網を形成するルータを設けるステップと、

を備えることを特徴とする通信制御方法。

【0185】

(付記19) 前記移動端末が、該第1のネットワークに接続した端末と通信を行う場合に、該移動端末と該端末との通信経路を最適化するステップを更に備えることを特徴とする付記18に記載の通信制御方法。

【0186】

(付記20) 前記ホームエージェントと、前記第1のネットワーク間には、予め仮想閉域網が設定されていることを特徴とする付記18に記載の通信制御方法。

【0187】

(付記21) 前記移動通信可能なプロトコルは、モバイルIPであることを特徴とする付記18に記載の通信制御方法。

(付記22) 前記ホームエージェントは、前記移動端末との間のモバイルIPのトンネル設定手順において、該移動端末に仮想閉域網に関する情報を通知し、該移動端末と該ルータ間に仮想閉域網を設定することを特徴とする付記21に記載の通信制御方法。

【0188】

(付記23) 前記モバイルIPと仮想閉域網の設定において、前記移動端末のcoo-1o c a t e dモードを利用することを特徴とする付記21に記載の通信制御方法。

【0189】

(付記24) 前記第2のネットワークは、公共ネットワークと、通信事業者の有する移動体通信網とからなり、前記移動端末がアクセスする該移動体通信網がセキュアなアクセス網である場合には、前記ホームエージェントと該移動端末との間にIP in IPのトンネルを設定することを特徴とする付記22に記載の通信制御方法。

【0190】

(付記25) 前記第2のネットワークは、公共ネットワークと、通信事業者の有する移動体通信網とからなり、前記移動端末がアクセスする該移動体通信網が非セキュアなアクセス網である場合には、前記ホームエージェントと該移動端末との間にIP S e cのトンネルを設定することを特徴とする付記22に記載の通信制御方法。

【0191】

(付記26) 前記第2のネットワークは、公共ネットワークと、第1の通信事業者の有する第1の移動体通信網と、第2の通信事業者の有する第2の移動体通信網とからなり、前記移動端末が該第1の移動体通信網から第2の移動体通信網と公共ネットワークを介して前記第1のネットワークにアクセスする場合、前記ルータと該移動端末との間にIP S e c + U D Pのトンネルを設定することを特徴とする付記22に記載の通信制御方法。

【0192】

(付記27) 前記ルータと前記第1のネットワークの間には、固定的な仮想閉域網を予め

設定しておくことを特徴とする付記１７に記載の通信制御方法。

（付記２８）移動端末とプライベートネットワークに接続された端末の通信を可能にするルータの通信制御方法であって、
該移動端末から送られてくる位置登録要求の気付けアドレスを検出するステップと、
該気付けアドレスが通信事業者が通信の秘匿性を確保可能なアクセス網を示している場合には、秘匿性の低い通信プロトコルで、該気付けアドレスが通信事業者が通信の秘匿性を十分保証しきれないアクセス網を示している場合には、秘匿性の高い通信プロトコルで、
該移動端末と該端末との通信を行わせる通信制御ステップと、
を備えることを特徴とするルータの通信制御方法。

【０１９３】

（付記２９）移動端末とプライベートネットワークに接続された端末の通信を可能にするルータの通信制御方法であって、
該移動端末から送られてくる位置登録要求の気付けアドレスと送信元アドレスを比較する比較ステップと、
該気付けアドレスが該送信元アドレスと一致する場合には、秘匿性の低い通信プロトコルで、該気付けアドレス該送信元アドレスと一致しない場合には、秘匿性の高い通信プロトコルで、該移動端末と該端末との通信を行わせる通信制御ステップと、
を備えることを特徴とするルータの通信制御方法。

【０１９４】

（付記３０）プライベートネットワークに接続された端末との通信を可能にする移動端末の通信制御方法であって、
該移動端末が現在自身の属する網の情報を取得する取得ステップと、
該取得した情報が、該網がプライベートネットワークであることを示す場合には、該移動端末の位置を管理するルータのプライベートなアドレスに位置登録要求メッセージを送出し、該アクセス網がプライベートネットワークと相互接続契約した通信事業者網であることを示す場合には、該ルータのグローバルなアドレスに位置登録要求メッセージを送出し、それ以外の場合には、該ホームページのグローバルなアドレスに、秘匿性の高い通信経路の設定要求を含む位置登録要求メッセージを送出するように制御する制御ステップと、
を備えることを特徴とする移動端末の通信制御方法。

【０１９５】

（付記３１）モバイルＩＰに従って移動端末とプライベートネットワークに接続された端末の通信を可能にするシステムにおける移動端末の通信制御方法であって、
モバイルＩＰの通信用トンネルを設定するステップと、
該モバイルＩＰの通信用トンネルの設定手順において、該プライベートネットワークの通信用トンネルを形成するステップとを備え、
該移動端末は、モバイルＩＰの通信用トンネルとプライベートネットワークの通信用トンネルを兼用した１つ通信用トンネルを使って通信を行うことを特徴とする移動端末の通信制御方法。

【０１９６】

【発明の効果】

本発明によれば、移動可能な第１の手段が移動しても通信可能なセッションの確立を行う手順の中で、仮想閉域網の設定をするので、移動可能な通信の設定と仮想閉域網の設定が一度にできる。従って、第１の手段が移動した結果、ハンドオフをする場合などにおいて、迅速に通信環境を整えることができるので、なめらかなハンドオフが実現できる。また、第１の手段は、第１のアドレスを固定的に保持して通信することができるので、どこの網に行っても、同じアドレスで通信できる。従って、第１の手段に送信しようとする場合、第１のアドレスを続けて使用可能となり、利便性が向上する。

【０１９７】

また、これを可能にするために、移動端末と自身との間に仮想閉域網を設定する手段を有

し、移動端末を認証することにより得られた、この仮想閉域網を設定するのに必要な情報を移動端末に通知して、移動端末が仮想閉域網内に入れるようにするホームエージェントが設けられるため、移動端末が別個に仮想閉域網内に入るための手順が不要となる。

【0198】

更に、移動端末が送信してくる気付けアドレスあるいはドメインから移動端末がいる網の秘匿性を検出し、秘匿性が弱い網の場合には、秘匿性の高い通信プロトコルを設定するので、重要な情報が漏れる可能性を少なくする。

【0199】

移動端末は、自身がいる網の情報を取得する手段を有し、自身がいる網の性質により、通信を開始するための通信プロトコルを変えることにより、やはり、重要な情報が漏れるのを防ぐことができる。

【0200】

特に、移動端末はネットワークとモバイルIP用トンネルとプライベートネットワークの通信用トンネルを兼用するので、ハンドオフが滑らかに行える。

【図面の簡単な説明】

【図1】本発明の機能ブロックである。

【図2】DIAMETERプロトコルの詳細を示す図（その1）である。

【図3】DIAMETERプロトコルの詳細を示す図（その2）である。

【図4】DIAMETERプロトコルの詳細を示す図（その3）である。

【図5】DIAMETERプロトコルの詳細を示す図（その4）である。

【図6】DIAMETERプロトコルの詳細を示す図（その5）である。

【図7】DIAMETERプロトコルの詳細を示す図（その6）である。

【図8】DIAMETERプロトコルの詳細を示す図（その7）である。

【図9】DIAMETERプロトコルの詳細を示す図（その8）である。

【図10】DIAMETERプロトコルの詳細を示す図（その9）である。

【図11】DIAMETERプロトコルの詳細を示す図（その10）である。

【図12】DIAMETERプロトコルの詳細を示す図（その11）である。

【図13】本発明の実施形態で使用するVPNデータベース17の構成を示す図である。

【図14】図1～図13で説明した機能を持つ認証サーバ及びネットワーク装置で構成されるIPネットワーク構成を示す図（その1）である。

【図15】図1～図13で説明した機能を持つ認証サーバ及びネットワーク装置で構成されるIPネットワーク構成を示す図（その2）である。

【図16】図1～図13で説明した機能を持つ認証サーバ及びネットワーク装置で構成されるIPネットワーク構成を示す図（その3）である。

【図17】図1～図13で説明した機能を持つ認証サーバ及びネットワーク装置で構成されるIPネットワーク構成を示す図（その4）である。

【図18】図1～図13で説明した機能を持つ認証サーバ及びネットワーク装置で構成されるIPネットワーク構成を示す図（その5）である。

【図19】図1～図13で説明した機能を持つ認証サーバ及びネットワーク装置で構成されるIPネットワーク構成を示す図（その6）である。

【図20】図1～図13で説明した機能を持つ認証サーバ及びネットワーク装置で構成されるIPネットワーク構成を示す図（その7）である。

【図21】AAAの機能ブロックを示す図である。

【図22】VPN情報キャッシュの構成を示す図である。

【図23】ルートテーブルの構成を示す図である。

【図24】AAAの処理フロー（その1）である。

【図25】AAAの処理フロー（その2）である。

【図26】AAAの処理フロー（その3）である。

【図27】HA、PCNの機能ブロックを示す図である。

【図28】VPN情報テーブルを示す図である。

- 【図29】MA (Mobile Agent) の処理フロー (その1) である。
- 【図30】MA (Mobile Agent) の処理フロー (その2) である。
- 【図31】MA (Mobile Agent) の処理フロー (その3) である。
- 【図32】MA (Mobile Agent) の処理フロー (その4) である。
- 【図33】MA (Mobile Agent) の処理フロー (その5) である。
- 【図34】MA (Mobile Agent) の処理フロー (その6) である。
- 【図35】MA (Mobile Agent) の処理フロー (その7) である。
- 【図36】MNの機能ブロックを示す。
- 【図37】MNの処理フロー (その1) である。
- 【図38】MNの処理フロー (その2) である。
- 【図39】MNの処理フロー (その3) である。
- 【図40】MNの処理フロー (その4) である。
- 【図41】MNの処理フロー (その5) である。
- 【図42】本発明の実施形態に従った、企業網内で通信する場合を説明する図 (その1) である。
- 【図43】本発明の実施形態に従った、企業網内で通信する場合を説明する図 (その2) である。
- 【図44】企業網内における経路の切り替え方を説明する図 (その1) である。
- 【図45】企業網内における経路の切り替え方を説明する図 (その2) である。
- 【図46】企業網内における経路の切り替え方を説明する図 (その3) である。
- 【図47】同一管理ドメイン内の拠点間通信について説明する図 (その1) である。
- 【図48】同一管理ドメイン内の拠点間通信について説明する図 (その2) である。
- 【図49】企業網内における経路切り替え方を説明する図 (その1) である。
- 【図50】企業網内における経路切り替え方を説明する図 (その2) である。
- 【図51】企業網内における経路切り替え方を説明する図 (その3) である。
- 【図52】同一管理ドメイン内の拠点間通信を説明する図 (その1) である。
- 【図53】同一管理ドメイン内の拠点間通信を説明する図 (その2) である。
- 【図54】PCN-PCN間の経路最適化方を説明する図 (その1) である。
- 【図55】PCN-PCN間の経路最適化方を説明する図 (その2) である。
- 【図56】PCN-PCN間の経路最適化方を説明する図 (その3) である。
- 【図57】移動通信事業者を介した通信について説明する図 (その1) である。
- 【図58】移動通信事業者を介した通信について説明する図 (その2) である。
- 【図59】移動通信事業者を介した通信について説明する図 (その3) である。
- 【図60】移動通信事業者網直結ホットスポットからの通信動作を説明する図 (その1) である。
- 【図61】移動通信事業者網直結ホットスポットからの通信動作を説明する図 (その2) である。
- 【図62】移動通信事業者網直結ホットスポットからの通信動作を説明する図 (その3) である。
- 【図63】ローミング提携先からの通信の動作を説明する図 (その1) である。
- 【図64】ローミング提携先からの通信の動作を説明する図 (その2) である。
- 【図65】ローミング提携先からの通信の動作を説明する図 (その3) である。
- 【図66】企業網内プロキシ経由によるインターネット接続の場合の動作を説明する図である。
- 【図67】移動通信業者網を介した通信の動作を説明する図 (その1) である。
- 【図68】移動通信業者網を介した通信の動作を説明する図 (その2) である。
- 【図69】移動通信業者網を介した通信の動作を説明する図 (その3) である。
- 【図70】移動通信事業者網直結ホットスポットからの通信の動作を説明する図 (その1) である。
- 【図71】移動通信事業者網直結ホットスポットからの通信の動作を説明する図 (その2) である。

）である。

【図72】移動通信事業者網直結ホットスポットからの通信の動作を説明する図（その3）である。

【図73】ローミング提携先からの通信の動作を説明する図（その1）である。

【図74】ローミング提携先からの通信の動作を説明する図（その2）である。

【図75】ローミング提携先からの通信の動作を説明する図（その3）である。

【図76】従来の技術における企業網と公共ネットワークを経由した通信を行う方法を説明する図である。

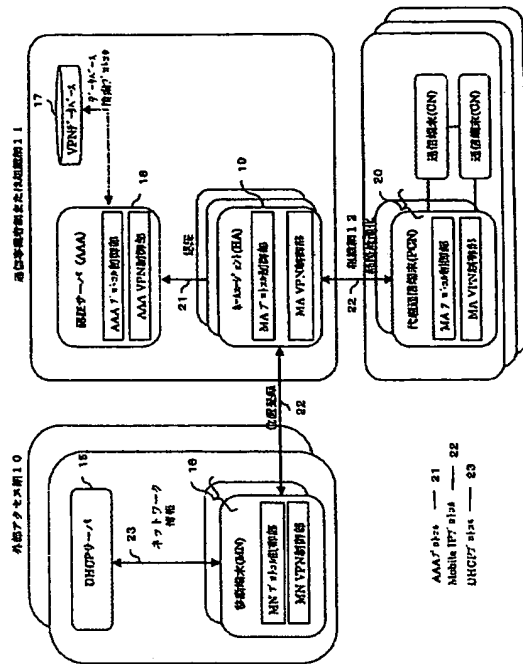
【図77】従来の技術における企業網と公共ネットワークを経由したシームレスな通信を行う方法を説明する図ある。

【符号の説明】

- 10 外部アクセス網
- 11 通信事業者網または企業網
- 12 企業網
- 15 DHCPサーバ
- 16 移動端末(MN)
- 17 VPNデータベース
- 18 認証サーバ(AAA)
- 19 ホームエージェント(HA)
- 20 代理CN(PCN)
- 30 AAAプロトコル制御部
- 31 AAAVPN制御部
- 32 アプリケーションサーバ
- 33 ネットワークカーネル
- 34 ネットワークデバイスインターフェース
- 35 AAAプロトコル処理部
- 36 VPN情報キャッシュ
- 37 鍵生成器
- 40 MAプロトコル制御部
- 41 MAVPN制御部
- 42 ネットワークカーネル
- 43 ネットワークデバイスインターフェース
- 44 AAAプロトコル処理部
- 45 モバイルIPプロトコル処理部
- 46 VPN情報キャッシュ
- 47 トンネル制御部
- 48 VPN情報テーブル
- 50 MNプロトコル制御部
- 51 MNVPN制御部
- 52 ネットワークカーネル
- 53 ネットワークデバイスインターフェース
- 54 モバイルIPプロトコル処理部
- 55 トンネル制御部
- 56 VPN情報テーブル
- 57 VPN情報キャッシュ
- 58 ルートテーブル

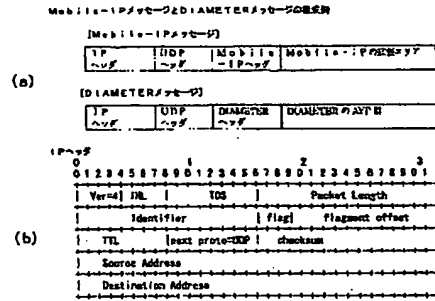
【図1】

本発明の機能ブロック



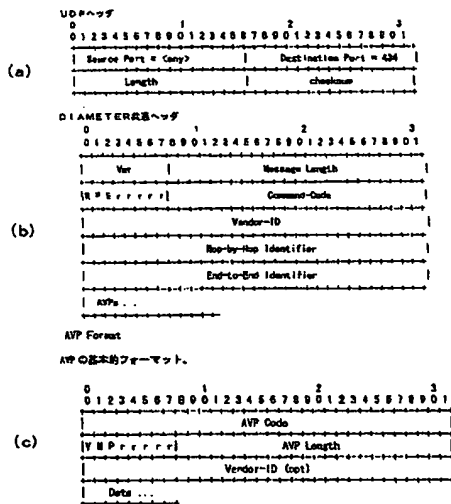
【図2】

DIAMETER プロトコルの詳細を示す図(その1)



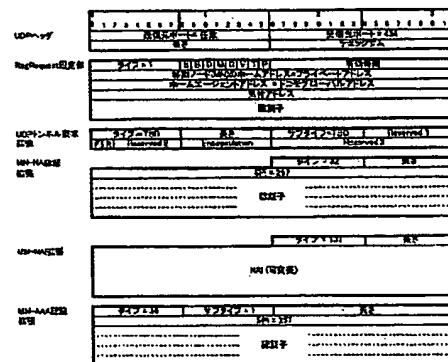
【図3】

DIAMETER プロトコルの詳細を示す図(その2)



【図4】

DIAMETERプロトコルの詳細を示す図(その3)



【図5】

DIAMETER プロトコルの詳細を示す図(その4)

(2) DIAMETERのAMRメッセージ構成

[illegible]

【图6】

DIAMETER プロトコルの詳細を示す図(その5)

(3) DIAMETERのHARメッセージ構成

[illegible]
















【图7】

DIAMETERプロトコルの詳細を示す図(その6)

[illegible]

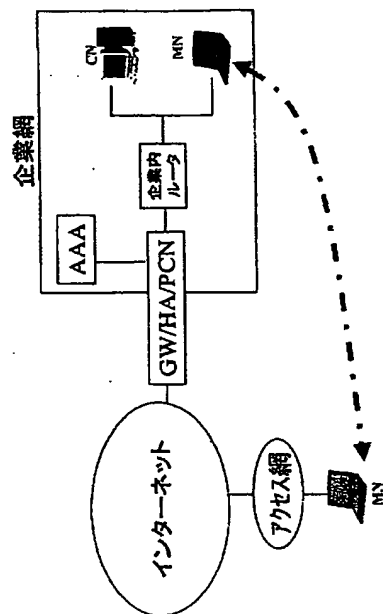
【图8】

DIAMETERプロトコルの詳細を示す図(その7)

<p>  </p> <p>  </p> <p>  </p>	<p>  </p> <p>  </p> <p>  </p>	<p>  </p> <p>  </p> <p>  </p>	<p>  </p> <p>  </p> <p>  </p>	<p>  </p> <p>  </p> <p>  </p>
--	---	--	--	--

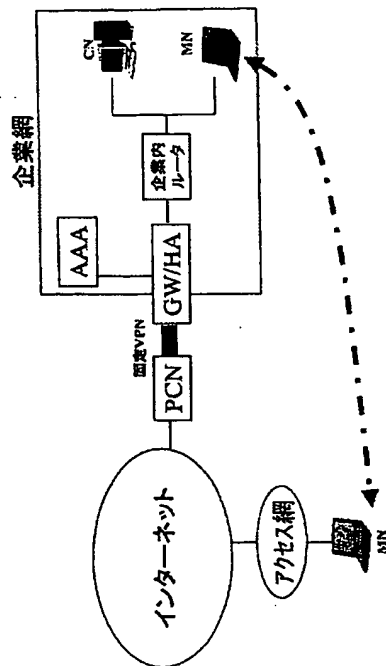
【图 14】

図1～図13で説明した機能を持つ認証サーバ及びネットワーク装置で構成されるIPネットワーク構成を示す図(その1)



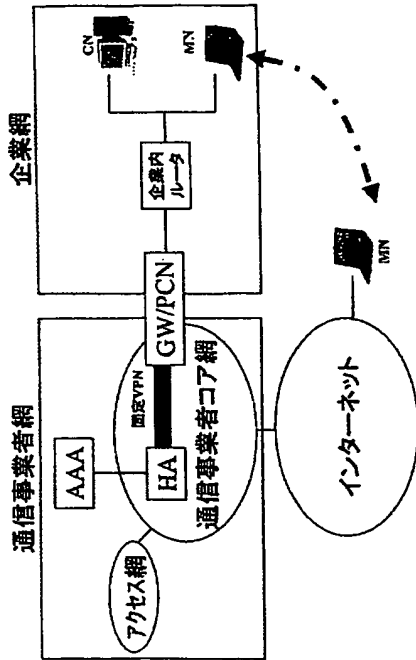
【图 16】

図1～図13で説明した機能を持つ認証サーバ及びネットワーク装置で構成されるIPネットワーク構成を示す図(その3)



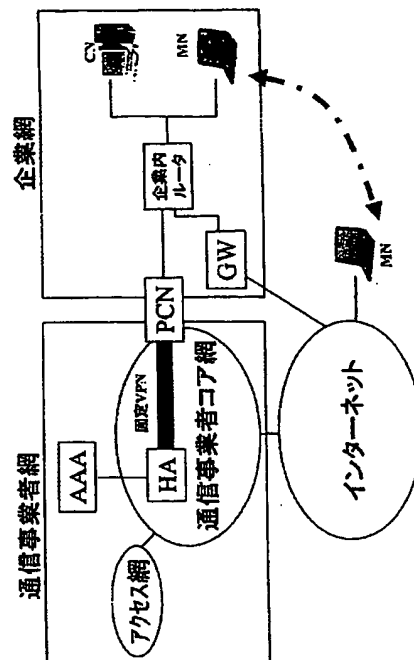
【図17】

図1～図13で説明した機能を持つ認証サーバ及びネットワーク装置で構成されるIPネットワーク構成を示す図(その4)



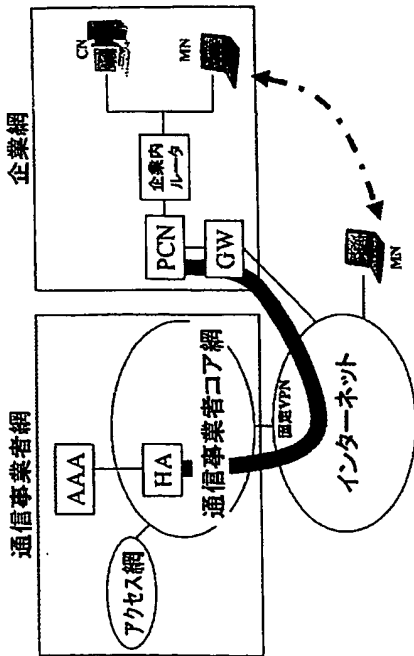
【図18】

図1～図13で説明した機能を持つ認証サーバ及びネットワーク装置で構成されるIPネットワーク構成を示す図(その5)



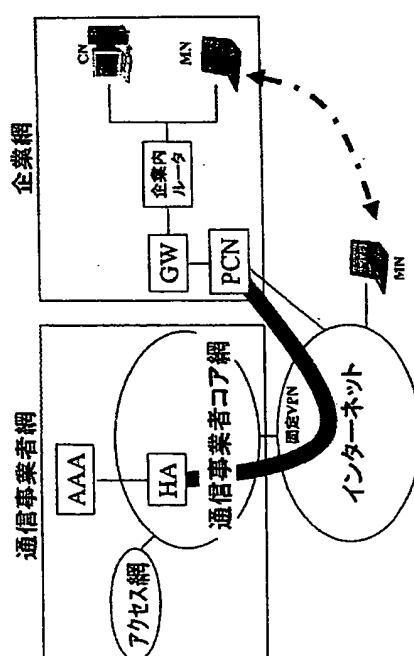
【図19】

図1～図13で説明した機能を持つ認証サーバ及びネットワーク装置で構成されるIPネットワーク構成を示す図(その6)



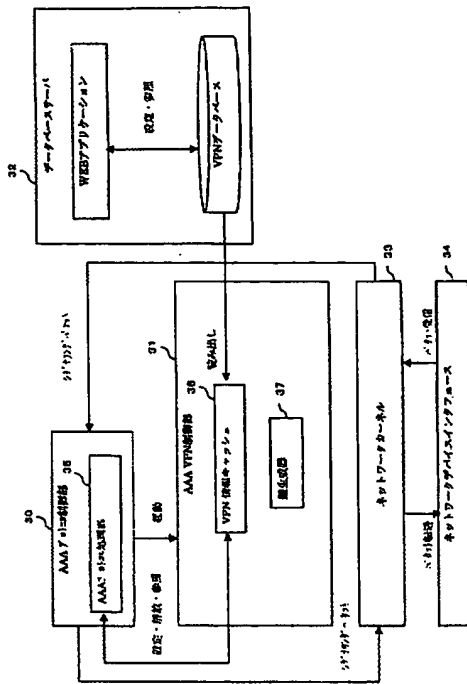
【図20】

図1～図13で説明した機能を持つ認証サーバ及びネットワーク装置で構成されるIPネットワーク構成を示す図(その7)



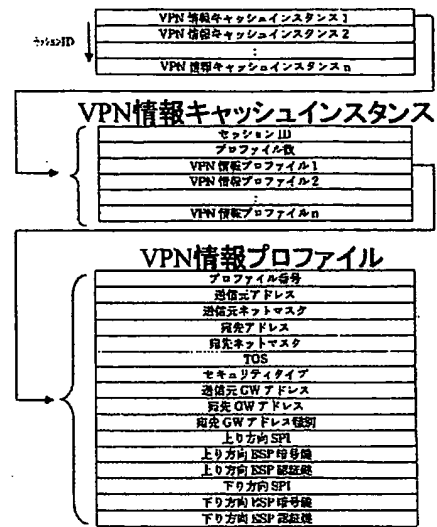
【図 2 1】

AAAの機能ブロックを示す図



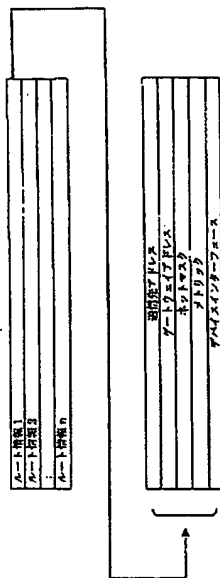
【図 2 2】

VPN情報キャッシュの構成を示す図



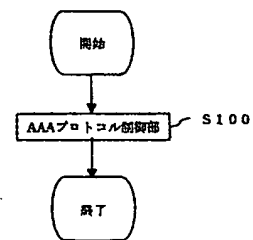
【図 2 3】

ルートテーブルの構成を示す図



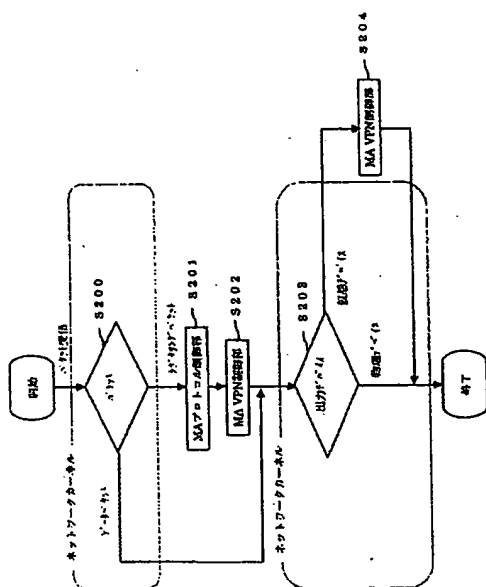
【図 2 4】

AAAの処理フロー(その1)



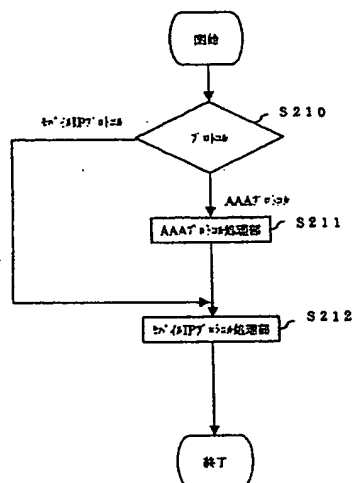
【図29】

MA(Mobile Agent)の処理フロー(その1)



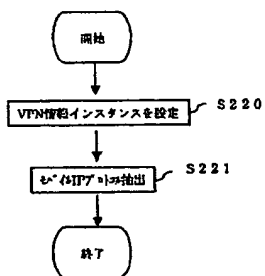
【図30】

MA(Mobile Agent)の処理フロー(その2)



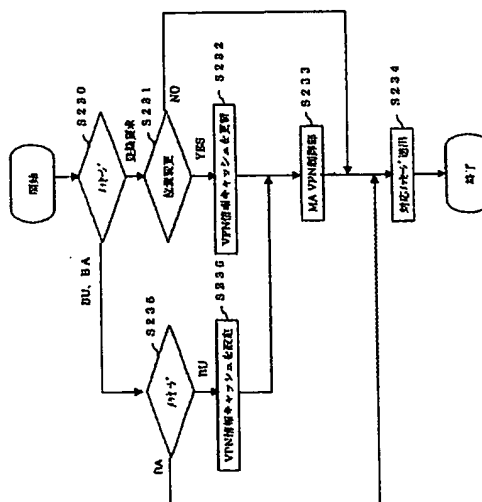
【図31】

MA(Mobile Agent)の処理フロー(その3)



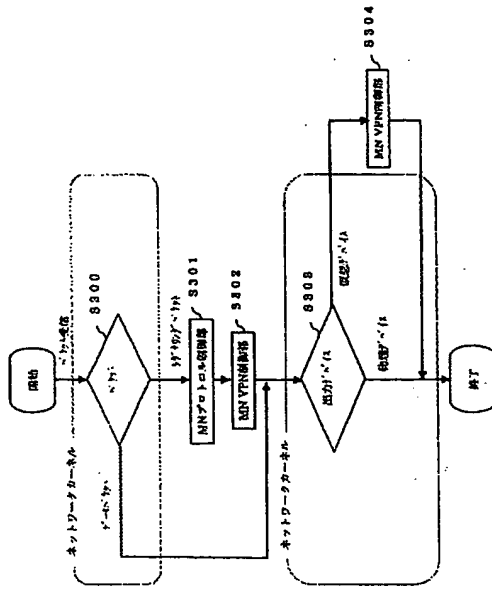
【図32】

MA(Mobile Agent)の処理フロー(その4)



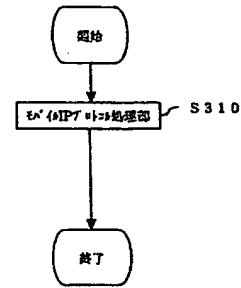
【図37】

MNの処理フロー(その1)



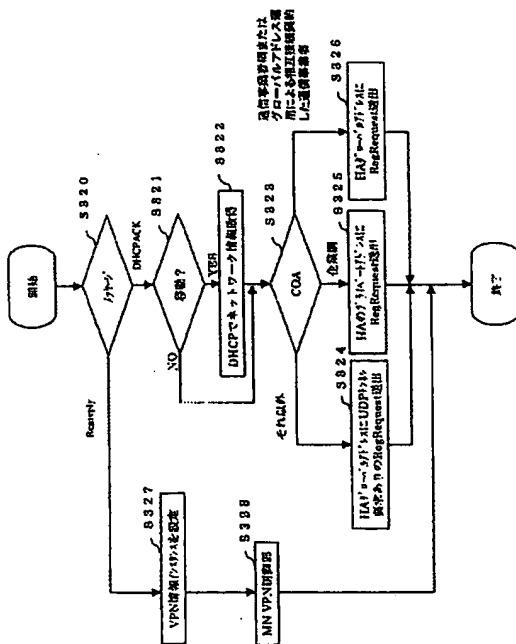
【図38】

MNの処理フロー(その2)



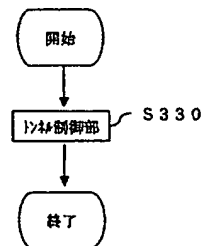
【図39】

MNの処理フロー(その3)



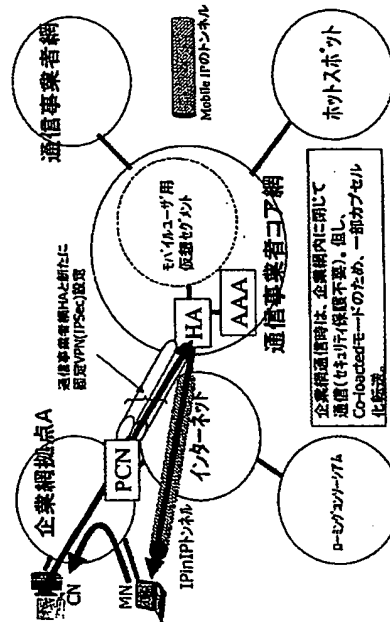
【図40】

MNの処理フロー(その4)



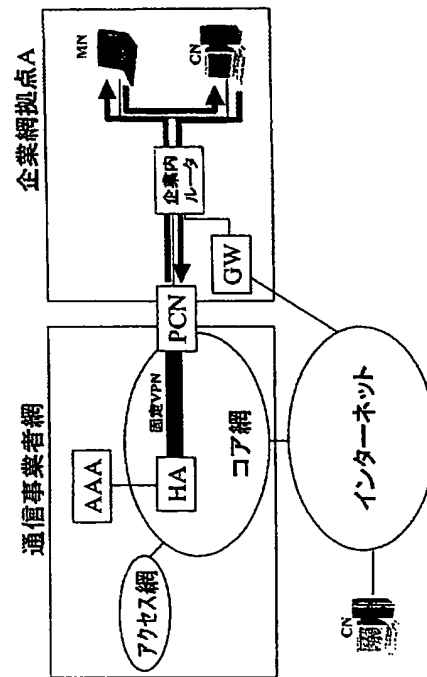
【図 4 2】

本発明の実施形態に従った、
企業網内で通信する場合を説明する図(その1)



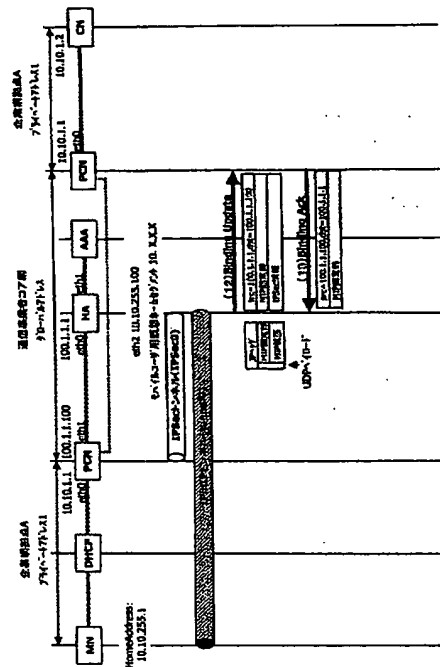
【图 4-4】

企業網内における経路の切り替え方式を説明する図(その1)



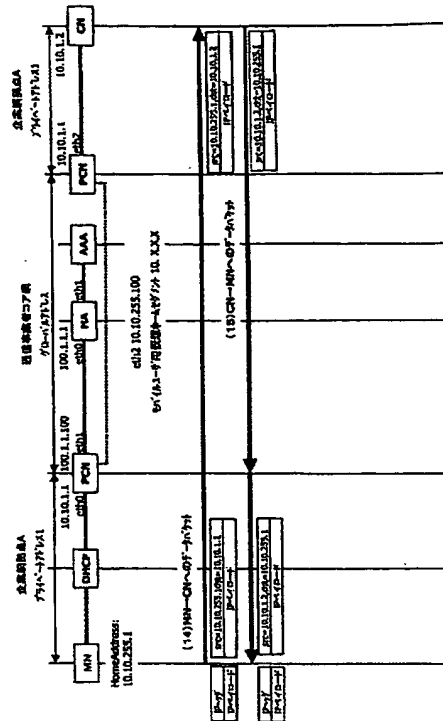
【図 45】

企業網内における経路の切り替え方式を説明する図(その2)



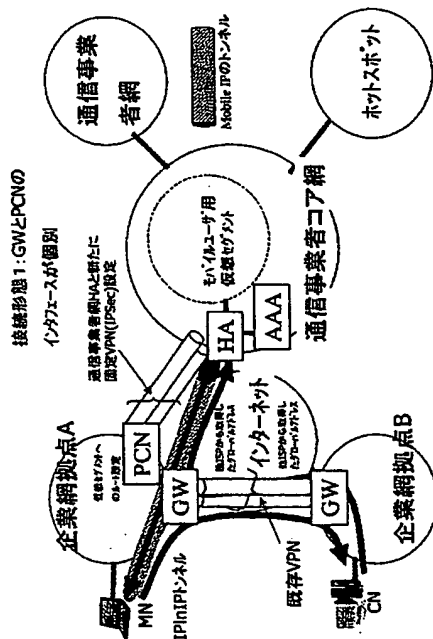
【図 46】

企業網内における経路の切り替え方式を説明する図(その3)



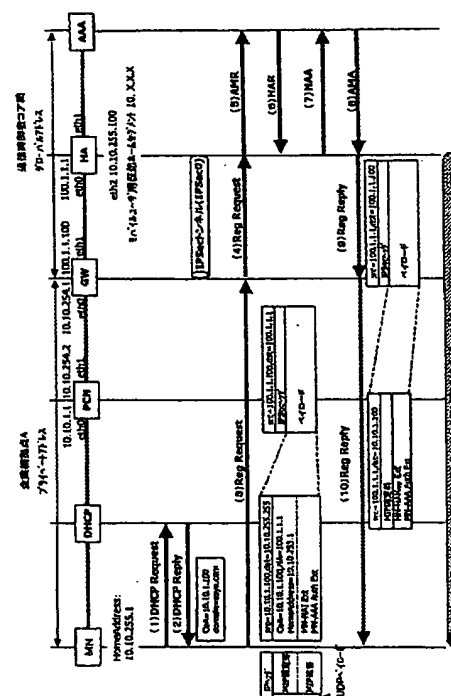
【図 47】

同一管理ドメイン内の拠点間通信について説明する図(その1)



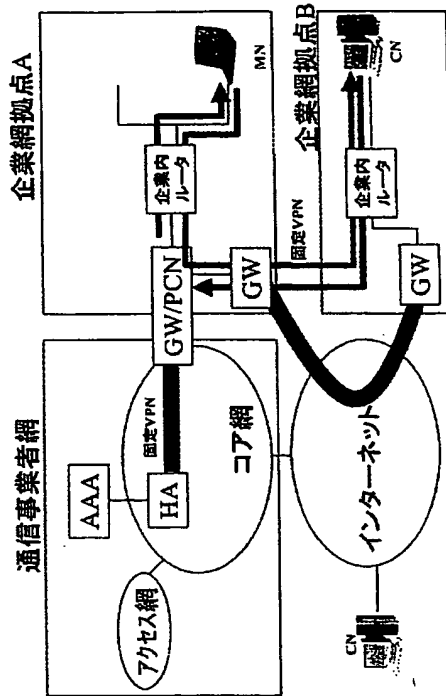
【図 48】

同一管理ドメイン内の拠点間通信について説明する図(その2)



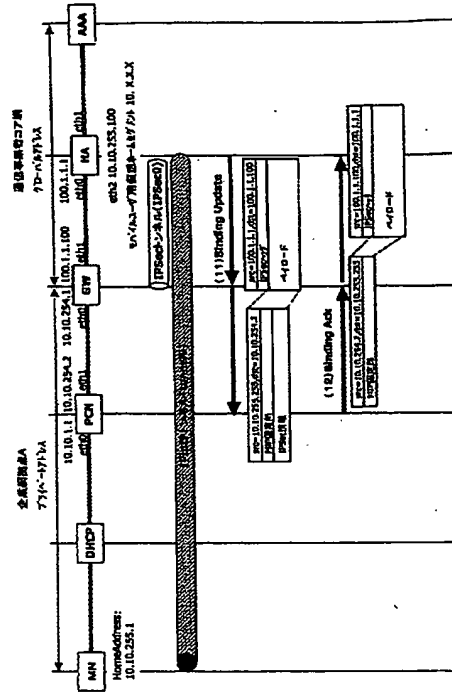
【図 49】

企業網内における経路切り替え方式を説明する図(その1)



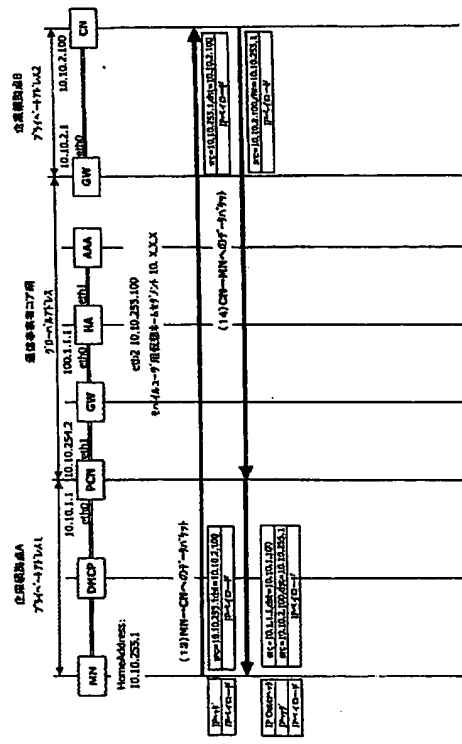
【図 50】

企業網内における経路切り替え方式を説明する図(その2)



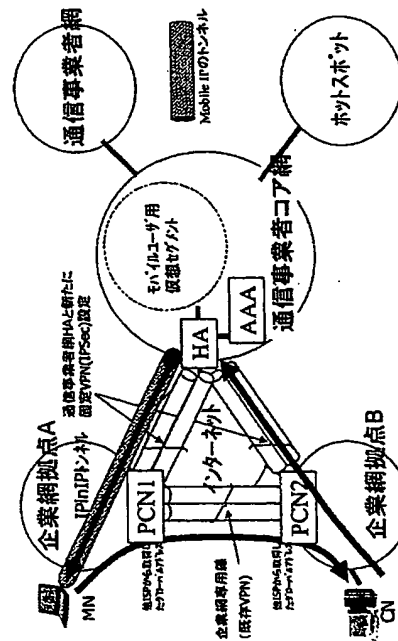
【図 51】

企業網内における経路切り替え方式を説明する図(その3)



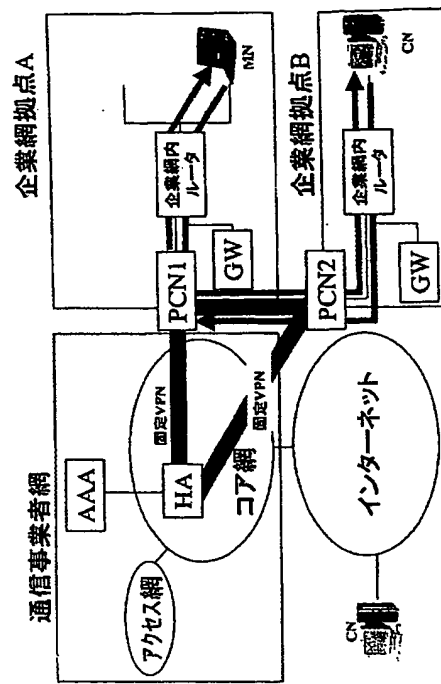
【図 52】

同一階層ドメイン内の拠点間通信を説明する図(その1)



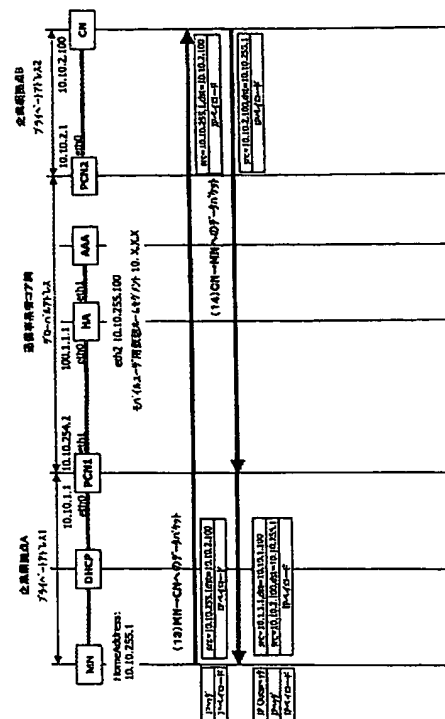
【图 5 4】

PCN-PCN間の経路最適化方式を説明する図(その1)



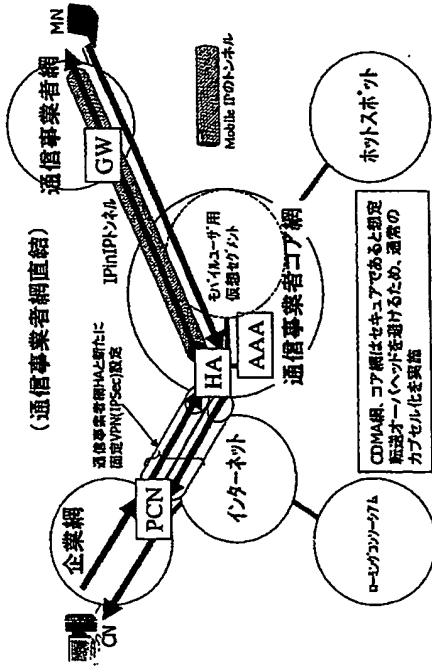
【图 5 6】

PCN-PCN間の経路最適化方式を説明する図(その3)



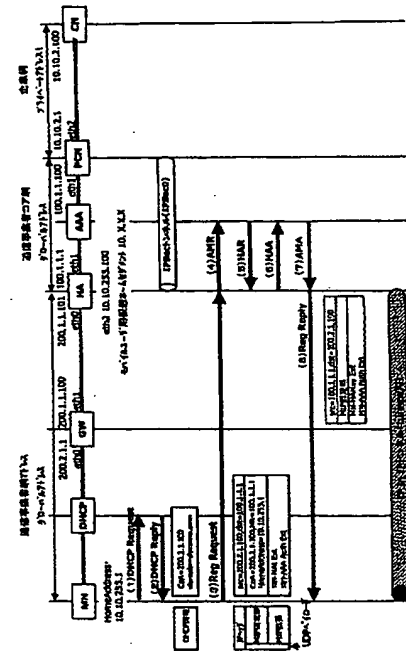
【図 57】

移動通信事業者を介した通信について説明する図(その1)



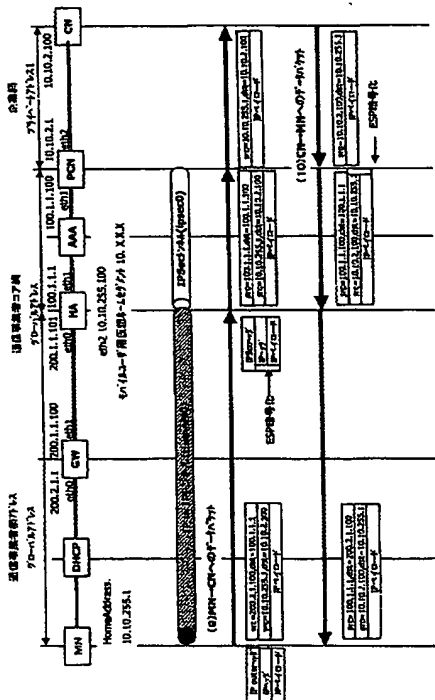
【図 58】

移動通信事業者を介した通信について説明する図(その2)



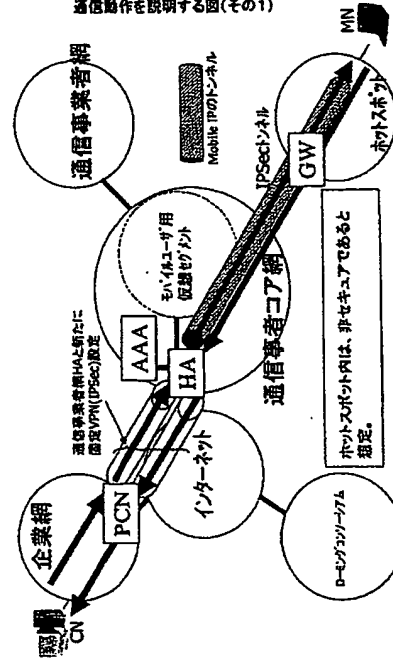
【図 59】

移動通信事業者を介した通信について説明する図(その3)

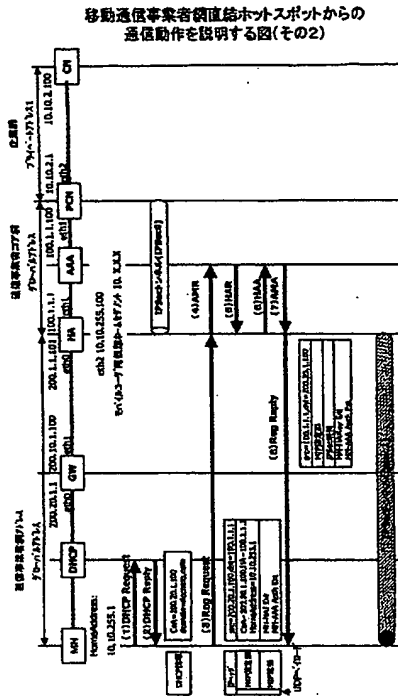


【図 60】

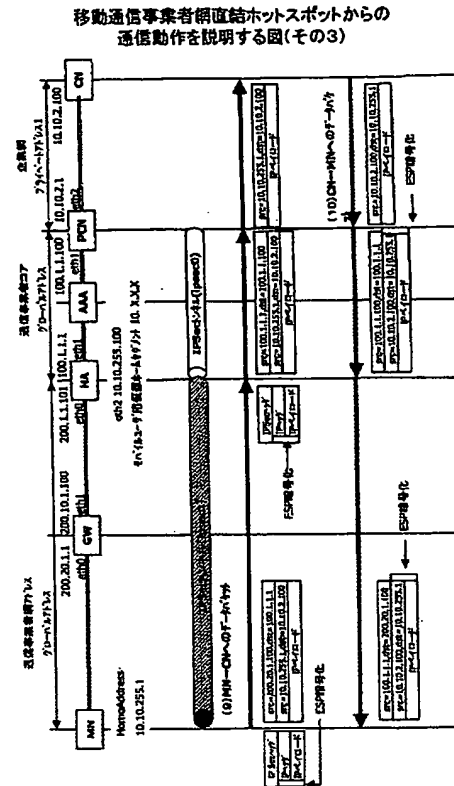
移動通信事業者網直結ホットスポットからの通信動作を説明する図(その1)



【図 6 1】

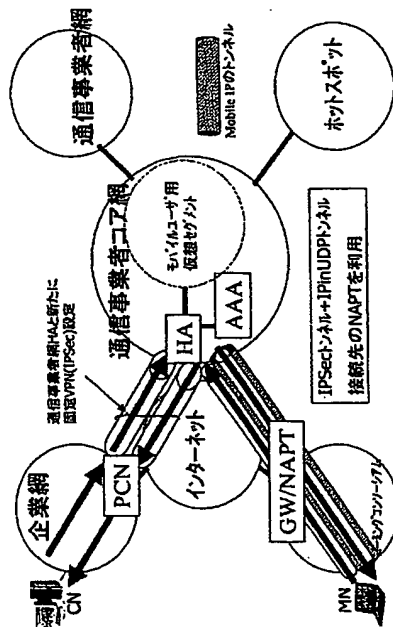


【図 6 2】



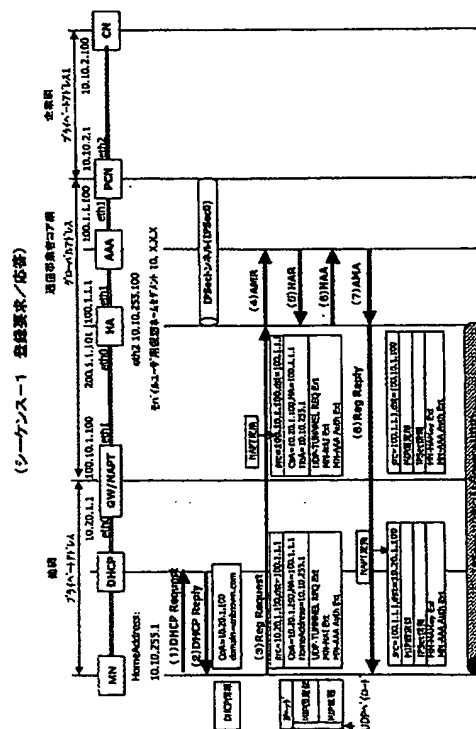
【図 6 3】

ローミング提供先からの通信の動作を説明する図(その1)



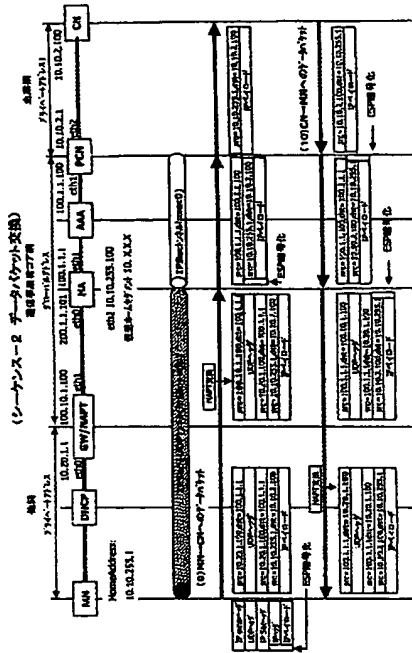
【図 6 4】

ローミング提供先からの通信の動作を説明する図(その2)



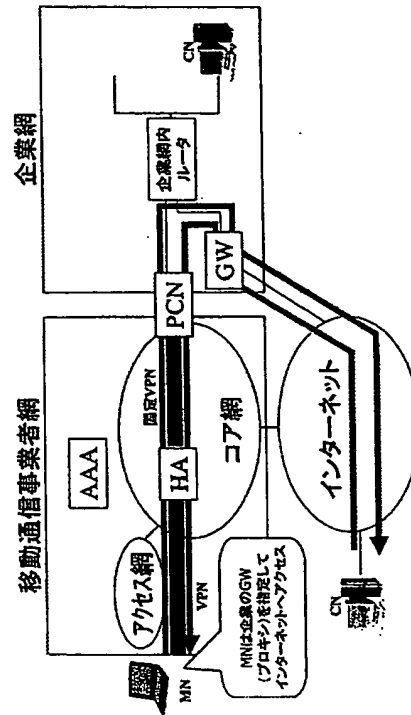
【図 65】

ローリング接続先からの通信の動作を説明する図(その3)



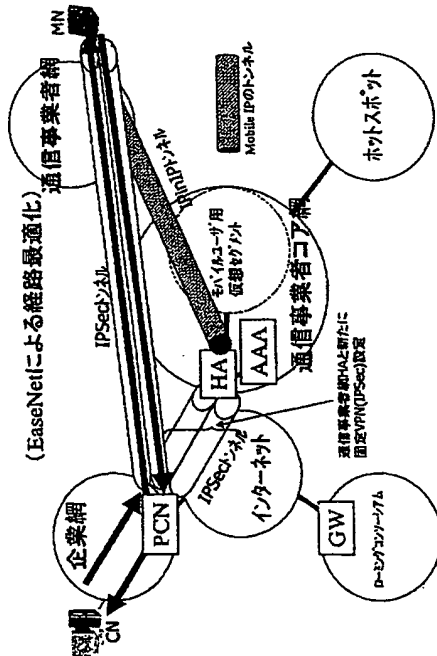
【図 66】

企業網内プロキシ経由によるインターネット接続の場合の動作を説明する図



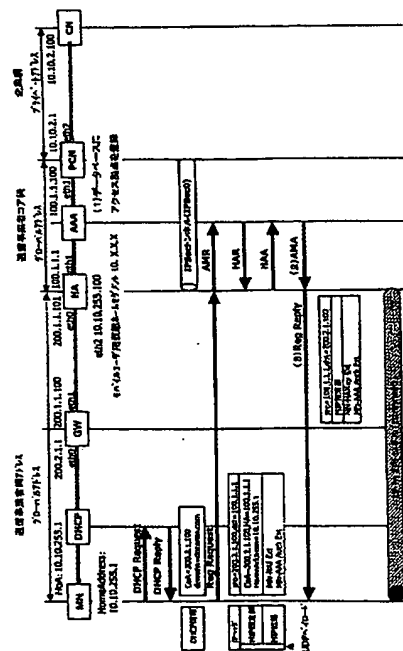
【図 67】

移動通信事業者網を介した通信の動作を説明する図(その1)



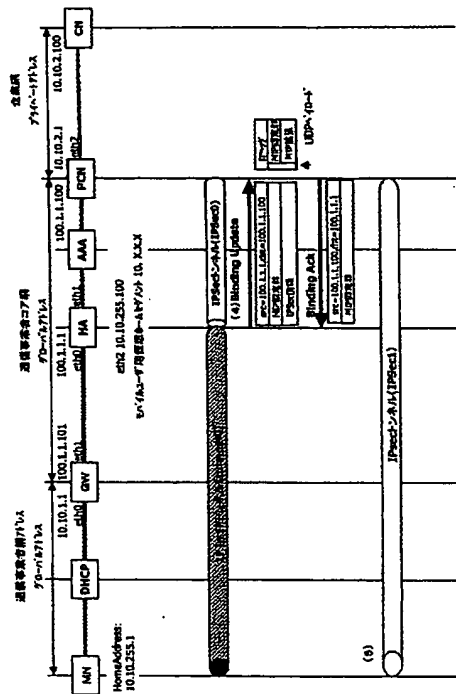
【図 68】

移動通信事業者網を介した通信の動作を説明する図(その2)



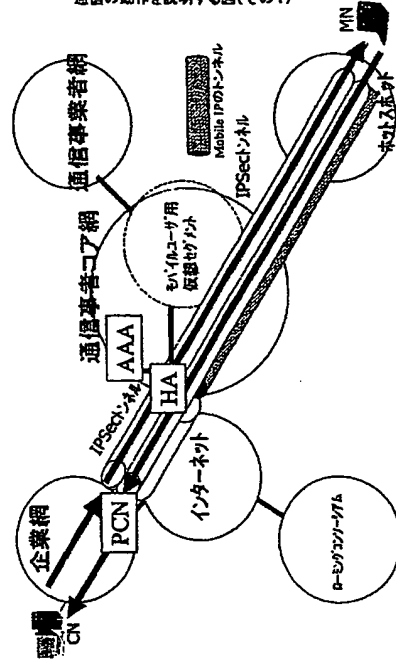
【図 69】

移動通信事業者網を介した通信の動作を説明する図(その3)



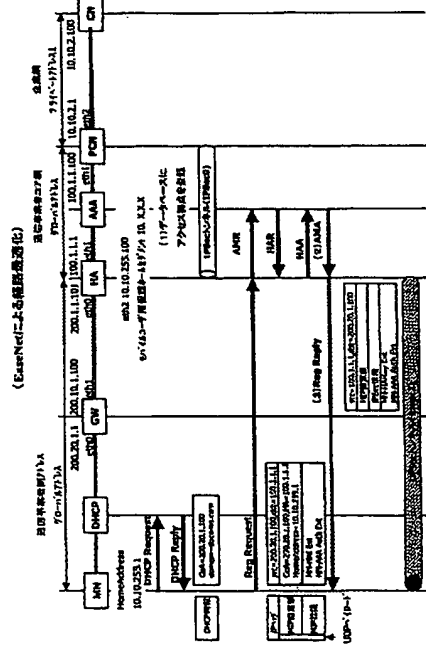
【図 70】

移動通信事業者網直結ホストスポットからの通信の動作を説明する図(その1)



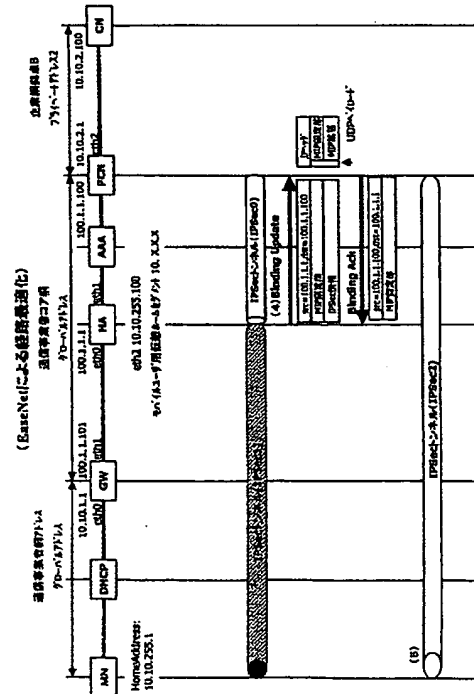
【図 71】

移動通信事業者網直結ホストスポットからの通信の動作を説明する図(その2)



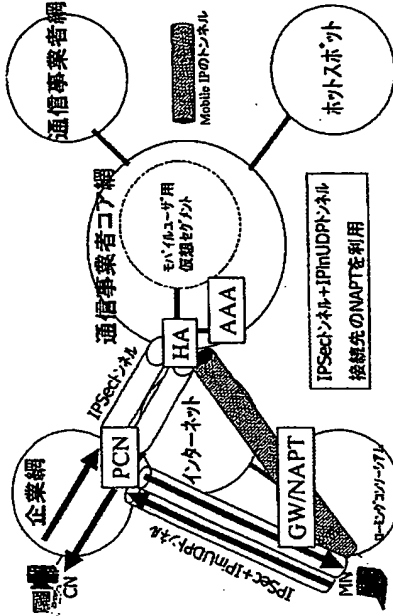
【図 72】

移動通信事業者網直結ホストスポットからの通信の動作を説明する図(その3)



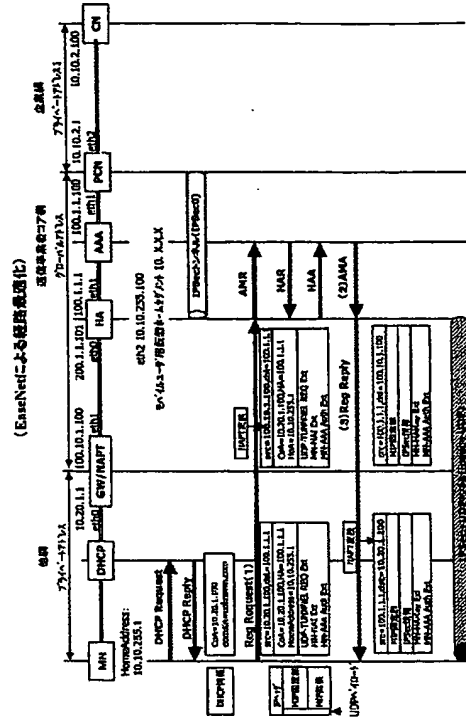
【図73】

ローミング提供先からの通信の動作を説明する図(その1)



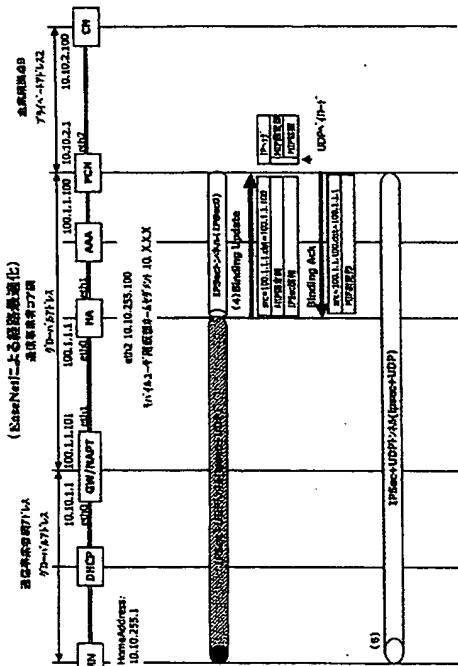
【図74】

ローミング提供先からの通信の動作を説明する図(その2)



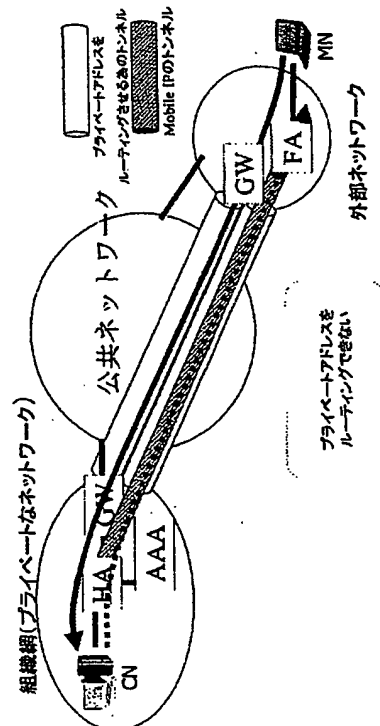
【図75】

ローミング提供先からの通信の動作を説明する図(その3)



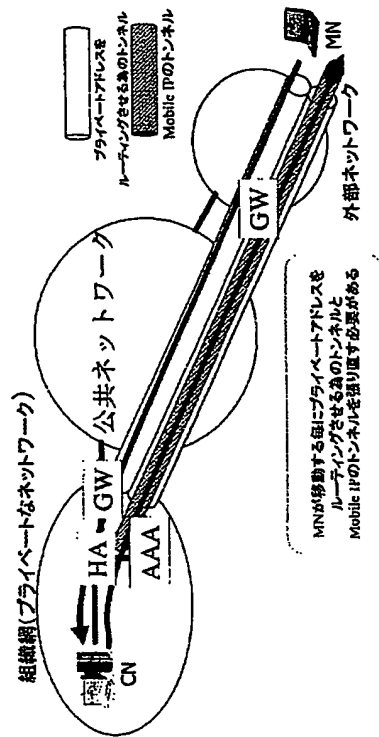
【図76】

従来の技術における企業網と公共ネットワークを経由した通信を行う方法を説明する図



【図 77】

従来の技術における企業網と公共ネットワークを経由した
通信を行う方法を説明する図



フロントページの続き

(72)発明者 若目田 宏

福岡県福岡市早良区百道浜2丁目2番1号 富士通西日本コミュニケーション・システムズ株式会社内

(72)発明者 谷口 浩之

神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

Fターム(参考) 5K030 HA08 HD06 HD09 JL01 JT09 LB05

5K033 DA06 DA19 DB18 EC03

5K067 BB21 DD17 EE02 EE10 EE16 GG01 GG11 HH22 HH23 HH24

JJ61 JJ70

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.